

? t s3/3

3/3/1 [Links](#)

Derwent WPI

(c) 2007 The Thomson Corporation. All rights reserved.

0012348951 *Drawing available*

WPI Acc no: 2002-291314/200233

Related WPI Acc No: 2004-794218

XRPX Acc No: N2002-227456

**Packet communication apparatus e.g. LAN switch, has state managers which receive directive packets to change state of network interfaces for forwarding packets**

Patent Assignee: HITACHI LTD (HITA); NOZAKI S (NOZA-I); SAWADA S (SAWA-I); WATANUKI T (WATA-I)

Inventor: NOZAKI S; SAWADA S; TATSUMI Y; WATANUKI T

Patent Family ( 3 patents, 2 countries )

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20020016858	A1	20020207	US 2001893004	A	20010628	200233	B
→ JP 2002084306	A	20020322	JP 2001195692	A	20010628	200236	E
→ US 6907470	B2	20050614	US 2001893004	A	20010628	200540	E

Priority Applications (no., kind, date): US 2001893004 A 20010628; JP 2000195706 A 20000629

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
US 20020016858	A1	EN	51	38		
JP 2002084306	A	JA	52			

Searching PAJ

1/2 ページ

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084306

(43)Date of publication of application : 22.03.2002

(51)Int.Cl.

H04L 12/46  
H04L 12/02  
H04L 12/22  
H04L 12/44  
H04L 12/56

(21)Application number : 2001-195692

(71)Applicant : HITACHI LTD

(22)Date of filing : 28.06.2001

(72)Inventor : SAWADA SUNAO  
WATANUKI TATSUYA  
NOZAKI SHINJI  
TATSUMI YOSHIYUKI

(30)Priority

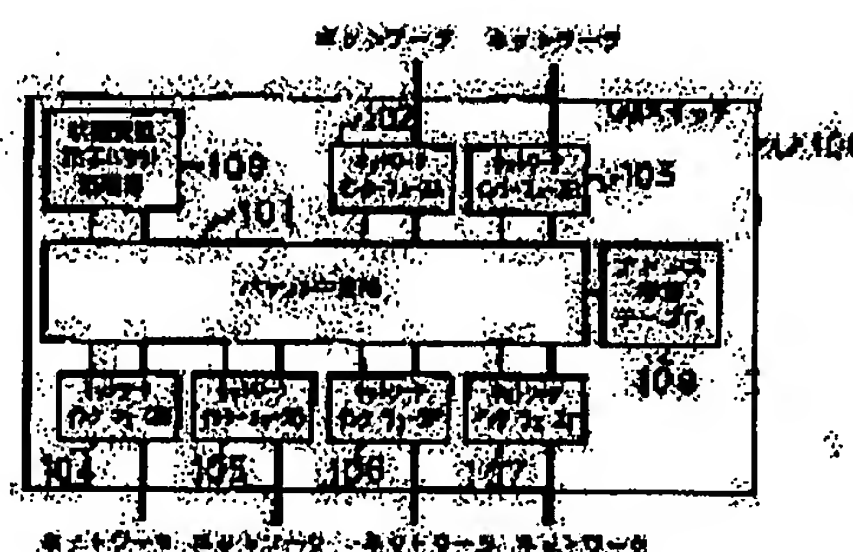
Priority number : 2000195706 . Priority date : 29.06.2000 Priority country : JP

## (54) PACKET COMMUNICATION APPARATUS AND NETWORK SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an unauthorized user from using a network system, in an unauthorized manner.

SOLUTION: A LAN 100 is provided with a packet relay part 101, a plurality of network interfaces 102 to 107, an address learning table 108 and a state change instruction packet processing part 109. In the processing part 109, a state change instruction packet which holds an instruction to change the state of a specific network interface to a 'connective state', a 'nonconnective state' or a 'no state' is received from an authentication server 401 via the part 101, and the state change instruction packet is transmitted to a state control part 203 inside the specific network interface. In the part 203, on the basis of the state change instruction packet, the state of the specific network interface is changed into the 'connective state', the 'nonconnective state' or the 'no state'.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-84306

(P2002-84306A)

(43) 公開日 平成14年3月22日 (2002.3.22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	特許庁 (参考)
H 0 4 L 12/46		H 0 4 L 12/46	M 5 K 0 3 0
	2 0 0		2 0 0 S 5 K 0 3 3
12/02		12/02	A
12/22		12/22	
12/44	3 0 0	12/44	3 0 0

審査請求 未請求 請求項の数 6 O L (全 52 頁) 最終頁に続く

(21) 出願番号 特願2001-195692(P2001-195692)

(22) 出願日 平成13年6月28日 (2001.6.28)

(31) 優先権主張番号 特願2000-195706(P2000-195706)

(32) 優先日 平成12年6月29日 (2000.6.29)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 澤田 素直

神奈川県秦野市堀山下1番地 株式会社日

立製作所エンタープライズサーバ事業部内

(72) 発明者 綿貫 達哉

神奈川県秦野市堀山下1番地 株式会社日

立製作所エンタープライズサーバ事業部内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

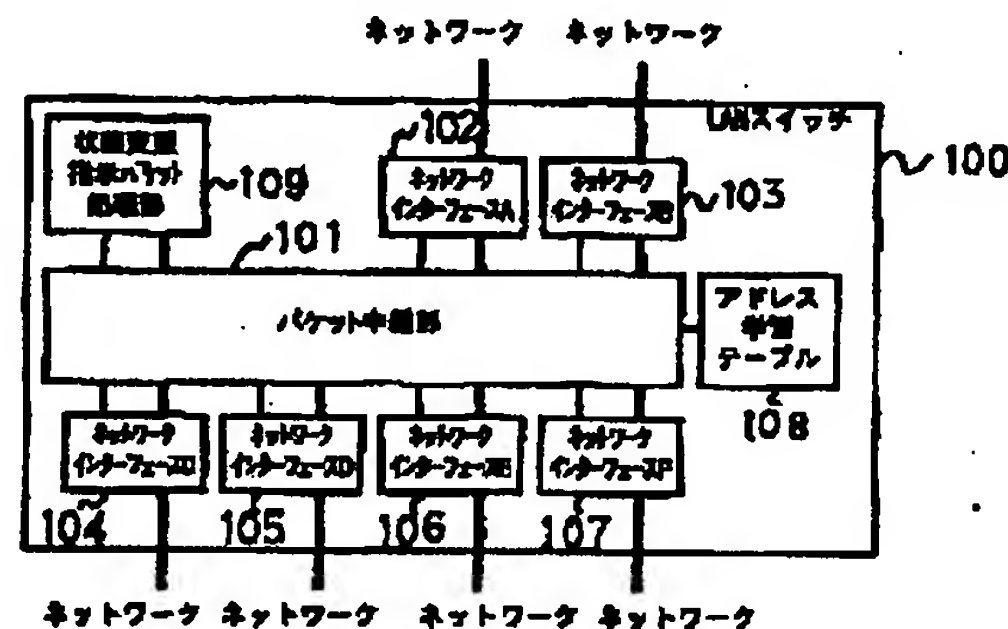
(54) 【発明の名称】 パケット通信装置及びネットワークシステム

(57) 【要約】

【課題】 不正なユーザがネットワークシステムを不正に利用することを防止する。

【解決手段】 LAN 100 は、パケット中継部 101、複数のネットワークインターフェース 102～107、アドレス学習テーブル 108 及び状態変更指示パケット処理部 109 を備え、状態変更指示パケット処理部 109 は、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継部 101 を介して認証サーバ 401 から受信すると共に、この状態変更指示パケットを、特定のネットワークインターフェース内の状態管理部 203 に送信する。この状態管理部 203 は、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する。

図 1



1

## 【特許請求の範囲】

【請求項1】 ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

複数のネットワークインターフェースと、  
パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、  
特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたパケット通信装置。

【請求項2】 前記ネットワークシステムでは、ネットワーク及びルータを介して配されたユーザ端末に動的にアドレスを配布するアドレス割り当てサーバをさらに備え、

受信したパケットの送信元アドレスを登録するフィルタリングテーブルをさらに備え、

前記状態変更指示パケット処理部は、  
前記フィルタリングテーブルに登録された特定のアドレスを、前記アドレス学習テーブルに登録するように指示する状態変更指示パケットを受信した場合、該特定のアドレスをアドレス学習テーブルに登録し、

パケットの宛先アドレスが、アドレス学習テーブルに登録されている場合、パケットを中継し、

パケットの宛先アドレスが、アドレス学習テーブルに未登録であり、かつ、前記フィルタリングテーブルに登録され、パケットの送信元アドレスが、ルータ又は認証サーバである場合、パケットを中継するようにした請求項1に記載のパケット通信装置。

【請求項3】 前記ネットワークインターフェースは、ネットワークが使用可能であるかどうかを検出する回線断検出部をさらに備え、

前記状態管理部は、

前記回線断検出部により回線断が検出された場合、回線断が検出されたネットワークインターフェースの状態を非接続状態に変更し、

(2)

特開2002-84306

2

前記認証サーバによりユーザ端末が認証を受けた場合、  
該ユーザ端末に接続されたネットワークインターフェースの状態を接続状態に変更し、

前記パケット中継部は、

非接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態又は接続状態のネットワークインターフェースには中継せず、特定のネットワークインターフェースにのみ中継し、

接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態のネットワークインターフェースには中継しないようにした請求項1又は2に記載のパケット通信装置。

【請求項4】 ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

20 パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部とを備えたパケット通信装置。

【請求項5】 ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、  
認証サーバにより認証を受けたユーザ端末のアドレスを登録するIPアドレス登録表と、

前記IPアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、IPアドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたパケット通信装置。

【請求項6】 請求項1乃至5のいずれかに記載のパケット通信装置と、

50 前記パケット通信装置にネットワークを介して接続され



3

たユーザ端末と、  
ファイルサーバと、  
前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための認証を行う認証サーバとを備えたネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、パケット通信装置及びネットワークシステムに係り、特に、LANスイッチやルータ等を用いてネットワークが不正に使用されることを防止する為のパケット通信装置及びネットワークシステムに関する。

【0002】

【従来の技術】近年、各種ネットワークが保持する情報に対する信用を確保するために、ネットワークの利用を制限する情報セキュリティ技術の必要性が認識されている。一方、ネットワークの利便性を考えて、例えば、IEEE (Institute of Electrical and Electronics Engineers, Inc.) で規定されているCSMA/CD (Carrier Sense Multiple Access with Collision Detection) 型の802.3ネットワークに代表されるLAN (Local Area Network) では、ネットワークに端末を接続しさえすれば使用できるようになっている。

【0003】また、IETF (Internet Engineering Task Force) で標準化されたDHCP (Dynamic Host Configuration Protocol) を用いれば、新たに接続された端末に対して自動的にアドレスが割り当てられ得る。これらのネットワークとノート型パソコンのような可搬型の端末により、端末の利用者が自由な場所で必要な時にネットワークを利用できる情報コンセントシステムが登場している。この情報コンセントシステムに関する技術としては、例えば、特開平11-68765号公報に記載されたものがある。

【0004】

【発明が解決しようとする課題】しかしながら、ネットワークの利用が容易になることで、ネットワークの使用許可を得ていない不正な利用者（不正ユーザ）であっても、ネットワークに端末を接続しさえすればネットワークを利用してしまふ場合が想定される。このため、ネットワークに接続されたファイルサーバなどの資源は、不正ユーザからの不正なアクセスにさらされるというセキュリティ上の不都合が生じる。

【0005】こうした不正ユーザによる不正なアクセスの防止に用いられる技術として、ルータ等のパケット通信装置による“パケットフィルタリング”が知られている。しかし、パケットフィルタリングの条件は予め設定しておかなければならない。それに対して、上述の情報コンセントシステムのように、任意の位置で動的に配布されたアドレスが端末により用いられるネットワークでは、予めパケットフィルタリングの条件を決めておくこ

(3)

特開2002-84306

4

とは困難である。

【0006】本発明は、以上の点に鑑み、不正ユーザがネットワークを不正に利用することを防止するパケット通信装置及びネットワークシステムを提供することを目的とする。

【0007】また、本発明は、ユーザがユーザ端末を自由な位置で、その度に違うアドレスを用いてネットワークに接続しても、そのユーザに対して許可されたネットワーク資源にしかそのユーザがアクセスできないパケット通信装置及びネットワークシステムを提供することを目的とする。

【0008】

【課題を解決するための手段】本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、複数のネットワークインターフェースと、パケットを送信すべきネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、学習テーブルを参照して、ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、特定のネットワークインターフェース内にそれぞれ設けられ、状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたパケット通信装置が提供される。

【0009】また、本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、ネットワークに接続するための物理インターフェースと、パケットの中継先を選択するパケット中継部と、パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、フィルタリングテーブルの内容に基づいて、パケットを廃棄又はパケット中継部に送信するパケット処理部とを有し、物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、フィルタリング処理部に対して、認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定されたフィルタリングテーブル内の情報を、認証サーバからの指示に基づいて変更し、認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットをファイル

## 5

サーバに中継するための情報を、フィルタリングテーブルに順次追加するフィルタリング変更指示処理部とを備えたパケット通信装置が提供される。

【0010】また、本発明によれば、ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるパケット通信装置であって、ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、認証サーバにより認証を受けたユーザ端末のアドレスを登録するIPアドレス登録表と、IPアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、IPアドレス登録表に未登録のアドレスを送信元アドレスとするパケットをカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたパケット通信装置が提供される。

【0011】本発明の特徴のひとつは、パケット通信装置が複数のネットワークインターフェースと、パケット中継部と、各ネットワークインターフェースが接続状態、非接続状態、状態なしのいずれの状態であるかを保持する状態管理部とを有することである。そして、各ネットワークインターフェースの状態がパケット中継部におけるパケットの中継先の選択に影響する。

【0012】本発明の他の特徴は、パケット通信装置が、状態変更指示パケット処理部を有し、状態変更指示パケットで指示されたネットワークインターフェースの状態を該状態変更指示パケットで指示された状態に変更することができることである。

【0013】本発明の他の特徴は、各ネットワークインターフェースが回線断検出部を有し、回線断検出部により回線断が検出されると、パケット通信装置はネットワークインターフェースの状態を非接続状態に変更することができることである。

【0014】本発明においては、初期化時に各ネットワークインターフェースの状態が非接続状態に初期化されるようにしてもよい。

【0015】本発明の他の特徴は、パケット通信装置が、非接続状態のネットワークインターフェースから受信したパケットを特定のネットワークインターフェースのみに中継することができることである。

【0016】本発明においては、パケット通信装置が、非接続状態のネットワークインターフェースから受信したパケットを、非接続状態あるいは接続状態のネットワークインターフェースに中継しないようにしてもよい。

【0017】本発明においては、パケット通信装置が、接続状態のネットワークインターフェースから受信したパケットを非接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【0018】本発明においては、認証を行ったユーザの使用端末が接続されたネットワークインターフェー

(4)

特開2002-84306

## 6

スの状態を、パケット通信装置が接続状態に変更するようにしてもよい。

【0019】本発明の他の特徴は、複数のネットワークインターフェース、パケット中継部、フィルタリングテーブル、フィルタリングテーブルの内容によってパケットフィルタリングを行うパケットフィルタリング部、及びフィルタリングテーブルの内容を外部からの指示により変更するフィルタリング変更指示処理部を有し、初期状態では全ての受信パケットを廃棄するようにフィルタリングテーブルの内容が設定されたパケット通信装置に対して、特定の送信元アドレスを持つパケットの中継を許可する内容を、外部からの指示によってフィルタリングテーブルに順次追加していくことができることである。

【0020】本発明においては、フィルタリングテーブルに順次追加していく内容は、認証を受けたユーザが使用する端末のアドレスを送信元アドレスとして持つパケットの中継許可を示す情報であってもよい。

【0021】本発明の他の特徴は、パケット通信装置が複数のネットワークインターフェース、パケット中継部、フィルタリングテーブル、アドレス学習テーブル及び状態変更指示パケット処理部を有し、受信したパケットの送信元アドレスをフィルタリングテーブルに登録し、フィルタリングテーブル内に登録された特定のアドレスをアドレス学習テーブルに登録するよう指示する状態変更指示パケットを受信した場合に、状態変更指示パケット処理部がフィルタリングテーブルに登録された特定のアドレスをアドレス学習テーブルに登録することである。

【0022】本発明において、パケット通信装置は、学習テーブルに登録されたアドレス宛のパケットを中継し、学習テーブルに登録されてなく、かつ、フィルタリングテーブルに登録されているアドレス宛のパケットについては、特定の送信元アドレスを有している場合にのみ中継することができるようにしてもよい。

【0023】本発明において、パケット通信装置は、認証を受けたユーザの使用端末のアドレスを学習テーブルに登録することを指示されることができる。

【0024】本発明において、パケット通信装置は、複数のネットワークインターフェース、パケット中継部、及びアドレス登録表を有し、アドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットについては、そのパケットをカプセル化した後、特定のアドレス宛に送信するようにしてもよい。

【0025】本発明において、パケット通信装置が、アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットをカプセル化して送信する際の宛先のアドレスは、ユーザの認証を行う装置のアドレスであ

7

ってもよい。

【0026】本発明において、パケット通信装置は、認証を受けたユーザの使用する端末のアドレスをアドレス登録表に登録するようにしてもよい。

【0027】本発明において、パケット通信装置の各ネットワークインターフェースが「非接続状態」かどうかを管理し、「非接続状態」である場合、通信を遮断するようにしてもよい。

【0028】本発明において、ネットワークから端末が離脱した場合、この離脱を検出したネットワークインターフェースが、自動的に「非接続状態」に切り替えるようにしてもよい。

【0029】本発明において、パケット通信装置が、ユーザに対して割り当てられたアドレスを把握し、この把握したアドレスに基づいてパケットフィルタリングの設定を行うようにしてもよい。

【0030】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を詳細に説明する。

【0031】図1は、本発明の一実施形態におけるパケット通信装置の構成図である。

【0032】LANスイッチ100は、例えば、パケット中継部101、複数のネットワークインターフェース102～107、アドレス学習テーブル108及び状態変更指示パケット処理部109を備える。ネットワークインターフェース102～107には、それぞれを一意に識別するために名前（図ではA～F）が割り当てられている。なお、名前は、一意に識別できれば番号等であってもよい。

【0033】これらのネットワークインターフェース102～107は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。なお、本実施の形態では、ネットワークとしてIEEEで規定されているCSMA/CD型の802.3ネットワークを、ツイストペア線で接続することを想定しているが、本発明は、その他のネットワーク（例えば無線ネットワーク）にも適用可能である。

【0034】パケット中継部101は、全てのネットワークインターフェース102～107と接続されており、OSI（Open System Interconnection）参照モデルのデータリンク層でパケット中継を行う。アドレス学習テーブル108には、パケット中継部101がパケットを送信すべきネットワークインターフェースを判断するために必要な情報が格納されている。

【0035】図3は、アドレス学習テーブル108の構成図（1）である。

【0036】アドレス学習テーブル108の各エントリは、アドレスフィールド301と送信ポートフィールド302を含む。アドレスフィールド301には、物理アドレス（以下、MACアドレスと記す）が、送信ポート

(5)

特開2002-84306

8

フィールド302には、ネットワークインターフェースの名前が、それぞれ格納される。ここで、アドレス学習テーブル108の各エントリは、パケットを中継する際、パケットの宛先アドレスがアドレスフィールド301に一致した場合、同じエントリの送信ポートフィールド302で示されるネットワークインターフェースから、パケットを送信することを表している。なお、送信ポートフィールド302には、複数のネットワークインターフェースを登録することができる。例えば、特殊なケースとして、LANスイッチ100自体のMACアドレスをアドレスフィールド301に登録し、送信ポートフィールド302を「X」とした場合、このエントリは、該当するパケットを、LANスイッチ100宛のパケットとして処理することを示している。

【0037】状態変更指示パケット処理部109は、LANスイッチ100に接続されたいずれかのネットワークを介して、外部（例えば、後述する認証サーバ401）よりLANスイッチ100宛に送られた状態変更指示パケットを、パケット中継部101を介して受信する。また、状態変更指示パケット処理部109は、この状態変更指示パケットの内容を適当なネットワークインターフェース102～107に通知する。状態変更指示パケットは、特定のネットワークインターフェースの状態を特定の状態に変更する指示を情報として保持している。なお、プロトコルとしては、例えば、SNMP（Simple Network Management Protocol）を使用するが、他にもtelnet（telecommunications network protocol）やHTTP（Hyper Text Transfer Protocol）などのプロトコルを利用してもよい。また、本実施の形態では、パケット通信装置としてLANスイッチ100を使用しているが、ルータ等その他のパケット通信装置に対しても、本発明は適用可能である。

【0038】図2は、ネットワークインターフェース102～107の構成図である。

【0039】ネットワークインターフェース102～107は、例えば、ネットワークに接続するための物理インターフェース201、ネットワークが使用可能であるかどうかを検出する回線断検出部202及びネットワークインターフェースの状態を管理する状態管理部203を備え、物理インターフェース201と状態管理部203は、パケット中継部101にそれぞれ接続されている。

【0040】回線断検出部202は、ネットワークの回線（ケーブル）が接続されているかどうか、又は回線を介して接続されている端末が使用可能な状態（電源投入状態）であるかどうかを電氣的に検出する。また、回線断検出部202は、検出された回線断を状態管理部203に通知する。本実施の形態では、回線断検出部202が回線断を検出するにあたって、物理インターフェース201から通知されるリンクダウン状態が100ms以



9

上続いた場合に、回線断と判定している。なお、回線として光ファイバを用いている場合は光信号の有無が、無線ならば電波の有無がそれぞれ同様に回線断の検出に使用できる。

【0041】状態管理部203は、ネットワークインターフェースの状態が「接続状態」、「非接続状態」及び「状態なし」のいずれであるかを管理する。ユーザ（スイッチ管理者）は、各ネットワークインターフェース102～107の状態管理部203に対して、常に「接続状態」または「状態なし」になるように予め設定することができる。各ネットワークインターフェース102～107の状態は、ユーザによる設定があればそのように、設定がなければ「非接続状態」となる。また、回線断検出部202により回線断が状態管理部203に通知されると、ユーザによる事前の設定がない場合、該当するネットワークインターフェースの状態は「非接続状態」になる。さらに、状態変更指示パケット処理部109による指示があった場合、その指示に基づいて該当するネットワークインターフェースの状態は上述の三つの状態のいずれかに変更される。

【0042】つぎに、図4に示されたネットワークシステムを例に、本発明に関するパケット通信装置を用いたネットワークシステムの動作を説明する。

【0043】図4は、本実施形態におけるLAN100を用いたネットワークシステムの構成図である。

【0044】このネットワークシステムは、例えば、LANスイッチ100（MACアドレス22:22:00:FF:FF:FF）と、LANスイッチ100のネットワークインターフェースA102に接続された認証サーバ401（MACアドレス22:22:00:11:11:11）と、ネットワークインターフェースB103に接続されたファイルサーバ402（MACアドレス22:22:00:22:22:22）と、ネットワークインターフェースC104～F107にそれぞれ接続され、ユーザが端末を自由に接続してネットワークを利用できる、いわゆる情報コンセント409と、情報コンセント409を介してネットワークインターフェースC104に接続されたユーザ端末403（MACアドレス22:22:FF:00:00:01）とを備える。

【0045】認証サーバ401は、ユーザがネットワークの使用を許可されているかどうかを判断し、その結果をLANスイッチ100に通知する。本実施の形態では、ユーザの認証を、ユーザIDとパスワードを用いて行う。また、LANスイッチ100の各ネットワークインターフェースC102～F107の設定は、ネットワークインターフェースB103は常に「接続状態」、ネットワークインターフェースA102は「状態なし」にそれぞれ設定し、ネットワークインターフェースC104～F107は特に設定をしない。したがって、ネット

(6)

特開2002-84306

10

ワークインターフェースC104～F107は、初期化時に「非接続状態」となる（なお、この際、LANスイッチ100の学習テーブル108は、図3に示すようになっている。）。

【0046】つぎに、このネットワークシステムにおいて、ユーザ端末403（MACアドレス22:22:FF:00:00:01）がネットワークインターフェースC104につながる情報コンセント409に接続された場合について説明する。

10 【0047】図5は、ユーザがユーザ端末403を情報コンセント409に接続した場合の通信シーケンス図である。

【0048】まず、認証を受けていないユーザ端末403が、ファイルサーバ402にアクセスする場合、ユーザ端末403から、宛先アドレスがファイルサーバ402のMACアドレス（22:22:00:22:22:22）、かつ、送信元アドレスがユーザ端末403のMACアドレス（22:22:FF:00:00:01）であるファイルサーバ宛パケット501が送信される。20 ここで、パケット501を受信したLANスイッチ100の中継処理を説明する。

【0049】図6は、パケット受信に対するLANスイッチ100の中継処理を示すフローチャートである。

【0050】パケット501を受信したLANスイッチ100のパケット中継部101は、学習テーブル108を参照する。パケット501に含まれた送信元アドレス（ユーザ端末403のMACアドレス22:22:FF:00:00:01）が学習テーブル108に登録されていなければ、パケット中継部101は、そのMACアドレスを学習テーブル108の1つのエントリにおけるアドレスフィールド301に登録する。また、パケット中継部101は、パケット501を受信したネットワークインターフェースの名前Cを送信ポートフィールド302に登録する。30

【0051】図7は、アドレス学習テーブル108の構成図（2）である。

【0052】学習テーブル108のエントリ#4におけるアドレスフィールドには、上述のように送信元アドレスとして、ユーザ端末403のMACアドレスが登録され、送信ポートフィールドには、ネットワークインターフェースCが登録される。40

【0053】つぎに、パケット中継部101は、宛先アドレスであるファイルサーバ402のMACアドレス（22:22:00:22:22:22）が学習テーブル108に登録済みであるので（処理602）、学習テーブル108のうちのファイルサーバ402の宛先アドレスが登録されているエントリの送信ポートフィールド302の内容に基づいて、パケット501を送信すべきポートとしてネットワークインターフェースBの情報を取得する（処理603）。そしてパケット中継部101 50



(7)

特開2002-84306

11

は、パケット501の中継処理を行う(処理604)。

【0054】ここで、処理604について説明する。

【0055】図8は、処理604のフローチャートである。

【0056】まず、パケット中継部101は、送信ポート(この場合ネットワークインターフェースB103)と受信ポート(この場合ネットワークインターフェースC104)とが同一かどうかを判定する(処理801)。ここでは、送信ポートと受信ポートは異なるポートであるので、後述する中継テーブル901に基づいて、パケット中継部101はパケット中継を行う(処理802)。

【0057】図9は、中継テーブル901の構成図である。

【0058】中継テーブル901は、受信ポートの状態と送信ポートの状態に基づいて、パケットの中継/廃棄を判定するために使用されるテーブルである。ここでは、ユーザ端末403から送信されたパケット501を受信するLANスイッチ100の受信ポート(ネットワークインターフェースC104)は「非接続状態」であり、送信ポート(ネットワークインターフェースB103)は「接続状態」であるので、中継テーブル901は「廃棄」を指示している。その結果、パケット501はパケット中継部101によって廃棄される。これにより、認証を受けていないユーザ端末403からのファイルサーバ402へのアクセスは回避されたことになる。

【0059】続いて、ユーザ端末403が、認証サーバ401に認証サーバ宛パケット502を送信する場合について説明する。

【0060】ユーザ端末403が、宛先アドレスが認証サーバ401のMACアドレス(22:22:00:11:11:11)であり、かつ、送信元アドレスがユーザ端末403のMACアドレス(22:22:FF:00:00:01)であるパケット502を送信する。このパケット502を受信したLANスイッチ100のパケット中継部101は、上述した図6に示されたフローチャートに従い中継処理を行う。

【0061】まず、学習テーブル108には、前回のパケット501受信時、ユーザ端末403のMACアドレス(22:22:FF:00:00:01)が既に登録されているので、パケット中継部101は処理601を通過する。つぎに、宛先アドレスである認証サーバ401のMACアドレス(22:22:00:11:11:11)が学習テーブル108に登録済みであるので(処理602)、学習テーブル108のうちの認証サーバ401の宛先アドレスが登録されているエントリの送信ポートフィールド302の内容に基づいて、パケット502を送信すべきポートとしてネットワークインターフェースAの情報を取得する(処理603)。そしてパケット中継部101は、パケット502の中継処理を行う

12

(処理604)。

【0062】ここで、再び、図8及び図9を用いて処理604について説明する。

【0063】まず、送信ポート(この場合はネットワークインターフェースA102)が受信ポート(この場合はネットワークインターフェースC104)とは異なるので(処理801)、処理802に進む。ここで、受信ポートであるネットワークインターフェースC104の状態は「非接続状態」、送信ポートであるネットワークインターフェースA102の状態は「状態なし」であるので、中継テーブル901は「中継」を示している。この結果、パケット502は、パケット中継部101によってネットワークインターフェースA102から認証サーバ401に中継される。

【0064】さらに、認証サーバ401からユーザ端末403への応答のパケット503は、同様に中継処理される。この場合、パケット503の受信ポートであるネットワークインターフェースA102の状態が「状態なし」、送信ポートであるネットワークインターフェースC104の状態が「非接続状態」であるので、中継テーブル901は「中継」を示す。従って、パケット503は、パケット中継部101によってネットワークインターフェースC104からユーザ端末403に中継される。つまり、認証サーバ401とユーザ端末403との間で双方向の通信が成立することになり、ユーザの認証が行われる。

【0065】認証サーバ401では、例えば、ユーザ端末403から送られてきたパケット502に含まれているユーザID及びパスワード504が、ネットワークの使用許可を与えられたユーザのものと一致した場合、LANスイッチ100に対して接続許可を通知する。この接続許可の通知には、宛先アドレスがLANスイッチ100のMACアドレス(22:22:00:FF:FF:FF)である状態変更指示パケット505が使用される。パケット505には、「接続状態への状態変更」とユーザ端末403のMACアドレス(22:22:FF:00:00:01)が情報として含まれている。

【0066】状態変更指示パケット505を受信したLANスイッチ100のパケット中継部101は、学習テーブル108を参照する。学習テーブル108において、状態変更指示パケット505の宛先アドレスであるLANスイッチ100自身のMACアドレスが登録されているエントリ中の送信ポートフィールド302は

「X」を示している(処理602)。従って、パケット505は、パケット中継部101により状態変更指示パケット処理部109に送られる(処理605)。状態変更指示パケット処理部109は、パケット505に含まれる情報からユーザ端末403のMACアドレス(22:22:FF:00:00:01)を取得すると共に、このMACアドレスを学習テーブル108のアドレ

13

スフィールド301から検索する。この検索によって得られた、ユーザ端末403のMACアドレスが登録されているエントリの送信ポートフィールド302に示されたネットワークインターフェース（この場合はC）に対して、状態変更指示パケット処理部109は、状態を「接続状態」に変更するように指示する。

【0067】ネットワークインターフェースC104においては、状態管理部203が状態を「非接続状態」から「接続状態」に変更する。この結果、ユーザ端末403からファイルサーバ宛パケット506を送信する場合、受信ポートとなるネットワークインターフェースC104が「接続状態」となる。この場合、送信ポートとなるネットワークインターフェースB103が「接続状態」であるため、中継テーブル901は「中継」を示す。これにより、ユーザ端末403からファイルサーバ402へのアクセスが可能となる。

【0068】次に、ユーザ端末403が情報コンセント409から離脱した場合のLANスイッチ100の動作を説明する。

【0069】ユーザが情報コンセント409からケーブル（ツイストペア線）を抜いてユーザ端末403の接続を解除すると、ネットワークインターフェースC104の物理インターフェース201が回線断の状態になる。その状態で100msが経過すると、回線断検出部202は、状態管理部203に回線断を通知する。回線断を通知された状態管理部203は、ネットワークインターフェースC104の状態を「非接続状態」に変更する。これにより、新たなユーザ端末が同じ情報コンセント409に接続された場合でも、あらためて認証を受けるまではそのユーザ端末はファイルサーバ402にアクセスできなくなる。

【0070】以上のように、本実施の形態のLANスイッチ100を用いることで、認証前のユーザ端末403からは、ファイルサーバ402へのアクセスが阻止され、認証後はアクセスが可能になり、さらに、ユーザ端末403の離脱後は、他のユーザ端末が再び認証を行うまではファイルサーバ402へのアクセスが阻止されるネットワークシステムを構築することができる。また、本実施の形態では、ユーザ端末403がネットワークインターフェースC104につながる情報コンセント409に接続された場合について説明したが、ネットワークインターフェースC104～F107の動作は同様であり、ユーザ端末403が任意の情報コンセント409に接続されても同様の効果が得られる。

【0071】また、本実施の形態では、ネットワークインターフェースの状態が、回線断により「非接続状態」に再初期化される。しかし、ユーザが離脱前に認証サーバ401と通信して離脱を通知し、その通知を受けた認証サーバ401が、「非接続状態に状態変更」を示す情報とユーザ端末403のMACアドレスとを含むパケッ

(8)

特開2002-84306

14

トを、LANスイッチ100のMACアドレス（22：22：00：FF：FF：FF）宛に送り、そのパケットを受信した状態変更指示パケット処理部109の指示により、ネットワークインターフェースの状態が「非接続状態」に変更されても構わない。この構成によれば、ユーザは、ユーザ端末403と情報コンセント409の接続を切らずに、ネットワークの使用可否を制御できる。図10は、パケット通信装置の他の構成を示す図である。

10 【0072】ルータ1000は、例えば、複数の物理インターフェース1002～1007、パケット中継部1001、複数のフィルタリング処理部1012～1017及びフィルタリング変更指示処理部1009を備える。物理インターフェース1002～1007は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。パケット中継部1001は、IP (Internet Protocol) プロトコルに基づいたパケット中継を行う。なお、本実施の形態では、パケット中継のプロトコルとしてIPプロトコル（IPv4 (IP version 4)）を用いるが、本発明は、例えば、IPv6 (IP version 6) など、その他のネットワーク層プロトコルにも適用可能である。また、本実施の形態では、パケット通信装置としてルータ1000を使用しているが、LANスイッチ等その他のパケット通信装置に対しても、本発明は適用可能である。

【0073】図11は、フィルタリング処理部1012～1017の構成図である。

【0074】フィルタリング処理部1012～1017は、フィルタリングテーブル1101、パケット処理部1102を備える。フィルタリングテーブル1101には、パケットの中継または廃棄の判断のための情報が格納されている。パケット処理部1102は、フィルタリングテーブル1101の情報に基づいて、パケットの廃棄又は、パケット中継部1001への送信を行う。パケット中継部1001に送られたパケットは、物理インターフェース1002～1007に送信される。各フィルタリングテーブル1101は、フィルタリング変更指示処理部1009と接続されており、フィルタリング変更指示処理部1009からの指示に応じてフィルタリングテーブル1101の内容を変更することができる。

40 【0075】図12は、フィルタリングテーブル1101の構成図（1）である。

【0076】フィルタリングテーブル1101は、パケットの中継または廃棄の判断のための情報を格納しており、各エントリは、宛先アドレス条件フィールド1201、送信元アドレス条件フィールド1202、中継／廃棄フラグフィールド1203を含む。宛先アドレス条件フィールド1201及び送信元アドレス条件フィールド1202には、IPアドレスまたは「任意」を意味する情報が登録されている。中継／廃棄フラグフィールド1

50

15

203には、パケットの宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件と送信元アドレス条件に一致した受信パケットを中継すべきか又は廃棄すべきかを示す情報が登録されている。複数のエントリの情報と一致するパケットがあった場合は、テーブルの先頭に近いエントリがそのパケットに適用される。また、一致するエントリが一つもないパケットは、フィルタリング処理部によりパケット中継部1001に送られる。

【0077】フィルタリング変更指示処理部1009は、後述される認証サーバ1311とネットワークを介して通信し、認証サーバ1311からフィルタリング変更指示を受ける。本実施の形態では、通信プロトコルとしてtelnetを想定するが、HTTPやCOPS

(Common Open Policy Service)などのプロトコルが使用されてもよい。フィルタリング変更指示は、対象とするエントリの内容と、追加/削除の指示を含む。フィルタリング変更指示処理部1009は、送信元アドレス条件フィールド1202に格納されているIPアドレスが属するサブネットに接続された物理インターフェース1002~1007に対応するフィルタリング処理部1012~1017のフィルタリングテーブル1101に、その指示を反映させる。

【0078】図13は、ルータ1000を用いたネットワークシステムの構成図である。

【0079】このネットワークシステムは、例えば、ルータ1000の各物理インターフェース1002~1007にそれぞれ接続されているサブネットA1302~F1307と、サブネットA1302に接続されている認証サーバ1311と、サブネットB1303に接続されているファイルサーバ1322と、サブネットC1304~F1307にそれぞれ接続され、ユーザが自由に端末を接続できる複数の情報コンセント409と、情報コンセント401を介してサブネットC1304に接続されているユーザ端末1333とを含む。

【0080】ルータ1000のフィルタリング処理部A1012、B1013における各フィルタリングテーブル1101には、初期状態では何も登録されていない。また、フィルタリング処理部C1014~F1017における各フィルタリングテーブル1101には、上述の図12に示されている内容と同じ内容がそれぞれ設定されている。

【0081】つぎに、このネットワークシステムで、ユーザ端末1333がサブネットC1304に接続された情報コンセント409に接続された場合について説明する。

【0082】図14は、ユーザによってユーザ端末1333が情報コンセント409に接続された場合の通信シーケンス図である。

【0083】認証を受けていないユーザ端末1333は、ファイルサーバ1322にアクセスするため、ファ

(9)

特開2002-84306

16

イルサーバ1322のIPアドレス(192.168.2.2)宛のファイルサーバ宛パケット1401を送信する。この場合、パケット1401は、ルータ1000の物理インターフェースC1004を介して、フィルタリング処理部C1014に送られる。図12に示されている通り、フィルタリング処理部C1014のフィルタリングテーブル1101のうち、宛先アドレス条件フィールド1201の内容が、パケット1401に含まれる宛先アドレスに該当するエントリは#2のエントリである。フィルタリング処理部C1014は、フィルタリングテーブル1101の#2のエントリを参照し、送信元アドレス条件フィールド1202や中継/排気フラグフィールド1203の内容を確認する。フィルタリングテーブル1101の#2のエントリの中継/排気フラグフィールド1203の内容は「廃棄」を示している。従って、フィルタリング処理部C1014は、フィルタリングテーブル1101の内容に従ってパケット1401を廃棄する。よって、認証を受けていないユーザ端末1333の送信するパケット1401は、ファイルサーバ1322に到達することはない。

【0084】つぎに、ユーザ端末1333が認証を受けてファイルサーバ1322にアクセスする場合の動作を説明する。

【0085】ユーザ端末1333は、認証を受けるために、認証サーバ1311のIPアドレス(192.168.1.1)宛のパケット1402を送信する。パケット1402は、ルータ1000の物理インターフェースC1004で受信され、フィルタリング処理部C1014に送られる。フィルタリング処理部C1014は、パケット1402に対して、フィルタリングテーブル1101の検索を行う。この場合、フィルタリングテーブル1101のエントリのうち#1、#2の両方のエントリの宛先アドレス条件フィールド1201の内容が、パケット1401に含まれる宛先アドレスに該当する。そこで、テーブル内の先頭に登録されている#1のエントリがパケット1402に適用される。フィルタリングテーブル1101の#1のエントリの中継/排気フラグフィールド1203の内容は「中継」を示している。このため、フィルタリングテーブル1101の#1のエントリを参照したフィルタリング処理部C1014は、中継/排気フラグフィールド1203の内容に従い、パケット1402をパケット中継部1001に送る。パケット1402は、パケット中継部1001によって物理インターフェースA1002から認証サーバ1311に中継される。これによって、ユーザ端末1333から認証サーバ1311への通信が成立する。

【0086】認証サーバ1311からユーザ端末1333へ送信された応答パケット1403は、物理インターフェースA1002により受信され、フィルタリング処理部A1012に送られる。フィルタリング処理部A1

50



17

012のフィルタリングテーブル1101には何も登録されていない。従って、パケット1403はフィルタリング処理部A1012からパケット中継部1001に送られる。パケット中継部1001は、物理インターフェースC1004からパケット1403をユーザ端末1333に送信する。これによって、ユーザ端末1333と認証サーバ1311との双方向の通信が成立することになり、ユーザ端末1333は、認証サーバ1311から認証を受けることができる。

【0087】パケット1403は、ユーザ端末1433に対してユーザID及びパスワードの送信を要求する。従って、パケット1403を受信したユーザ端末1333に対してユーザはユーザID及びパスワードを入力する。入力されたユーザIDとパスワードを含むパケット1404が、ユーザ端末1333から認証サーバ1311に送られる。パケット1404は、上述のようにしてルータ1000により中継され、認証サーバ1311に受信される。認証サーバ1311は、ユーザ端末1333から送られてきたパケット1404に含まれるユーザIDとパスワードが、ネットワーク接続を許可されたユーザのものとは一致した場合、ルータ1000のフィルタリング変更指示処理部1009と通信し、フィルタリングテーブル1101に対して、宛先アドレス条件フィールド1201の内容が「任意」、送信元アドレス条件フィールド1202の内容がユーザ端末1333のIPアドレスである「192.168.3.3」、中継/廃棄フラグフィールド1203の内容が「中継」であるエントリを追加することを指示1405する。

【0088】図15は、フィルタリングテーブル1101の構成図(2)である。

【0089】フィルタリング変更指示処理部1009は、認証サーバ1311から指示された送信元アドレス条件「192.168.3.3」が属するサブネット(サブネットC1304)が物理インターフェースC1004に接続されている為、フィルタリング処理部C1014のフィルタリングテーブル1101に対して、指示されたエントリを追加する。その結果、図15に示されるように、フィルタリング処理部C1014のフィルタリングテーブル1101には、新たなエントリが#1のエントリとして追加され、#1~#3までのエントリがフィルタリングテーブル1101に登録されていることになる。

【0090】その後、ユーザ端末1333がファイルサーバ1322宛のパケット1406を送信した場合、パケット1406に含まれる送信元アドレスがフィルタリング処理部C1014のフィルタリングテーブル1101における#1のエントリの送信元アドレス条件に該当する。このため、パケット1406はフィルタリング処理部C1014からパケット中継部1001に送られ、ファイルサーバ1322に中継される。この結果、ユー

(10)

特開2002-84306

18

ザ端末1333からファイルサーバ1322へのアクセスが可能となる。

【0091】以上のように、ルータ1000を用いることで、認証サーバ1311による認証を受けていないユーザ端末1333からファイルサーバ1322へのアクセスは阻止され、ユーザ端末1333が認証を受けた後、ユーザ端末1333からファイルサーバ1322へのアクセスが許可されるネットワークシステムを構築することができる。また、ルータ1000の各物理インターフェース1002~1007は複数の情報コンセント409を扱うことができる。さらに、物理インターフェースごとに個別のフィルタリング処理部が設けられることにより、ルータ1000においてフィルタリング処理の負荷を分散することができる。

【0092】図16は、パケット通信装置の他の構成を示す図である。

【0093】LANスイッチ1600は、例えば、パケット中継部1601、複数のネットワークインターフェース1602~1605、アドレス学習テーブル1606、フィルタリングテーブル1607及び状態変更指示パケット処理部1608を備える。ネットワークインターフェース1602~1605には、各々を一意に識別するために名前(図ではA~D)が割り当てられている。なお、名前は、一意に識別できれば番号等であってもよい。

【0094】これらのネットワークインターフェース1602~1605は、それぞれ異なるネットワークに接続されており、パケットの送受信を行う。なお、ネットワークは、IEEEの802.3ネットワークである。また、以下の説明では、ネットワークインターフェースA1602を「アップリンク」、ネットワークインターフェースB1603~D1605を「ダウンリンク」と称する。

【0095】パケット中継部1601は、アドレス学習テーブル1606とフィルタリングテーブル1607が保持する情報に基づいて、ネットワーク間でのパケット中継を行う。状態変更指示パケット処理部1608は、後述する認証サーバ1901からの状態変更指示パケットを受信し、フィルタリングテーブル1607と学習テーブル1606の内容を変更する。状態変更指示パケットには、IPアドレスと「許可/禁止」を示す情報とが含まれる。

【0096】図17は、フィルタリングテーブル1607の構成図である。

【0097】フィルタリングテーブル1607には、中継が許可されていないパケットを識別するための情報が登録されている。フィルタリングテーブル1607の各エントリは、MACアドレスフィールド1701、IPアドレスフィールド1702、接続ポートフィールド1703を含む。MACアドレスフィールド1701に

50



19

は、フィルタリング対象となるMACアドレスが、IPアドレスフィールド1702には、そのMACアドレスに対応するIPアドレスが、接続ポートフィールド1703には、そのMACアドレスを持つユーザ端末が属するネットワークに接続されているネットワークインターフェース1602～1605の名前が、それぞれ登録されている。

【0098】図18は、学習テーブル1606の構成図(1)である。

【0099】学習テーブル1606には、パケットの中継先ネットワークインターフェースに関する情報が登録されている。学習テーブル1606の各エントリは、MACアドレスフィールド1801及び接続ポートフィールド1802を含む。MACアドレスフィールド1801には、中継対象となるMACアドレスが、接続ポートフィールド1802には、パケットに含まれる宛先MACアドレスがMACアドレスフィールドの内容に一致したパケットを中継すべきネットワークインターフェース1602～1605の名前が、それぞれ登録されている。また、一定時間利用されなかったエントリは、自動的に学習テーブル1606から削除されるように設定されている。

【0100】次に、図19に示されたネットワークを例に、LANスイッチ1600を用いたネットワークシステムの動作を説明する。

【0101】図19は、LANスイッチ1600を用いたネットワークシステムの構成図である。

【0102】このネットワークシステムは、例えば、LANスイッチ1600と、LANスイッチ1600の各ネットワークインターフェース1602～1605にそれぞれ接続されたネットワークA～Dと、ネットワークB～Dを介して、ダウンリンクの各ネットワークインターフェースB1603～D1605に接続された、ユーザが自由に端末を接続できる複数の情報コンセント409と、情報コンセント409を介してネットワークBに接続されたユーザ端末1905と、ネットワークAを介してアップリンクのネットワークインターフェースAに接続されたルータ1904と、ネットワークを介してルータ1904に接続されたファイルサーバ1902、DHCPサーバ1903、認証サーバ1901とを含む。

【0103】ルータ1904は、BOOTPリレーエージェント機能を備え、IPプロトコルに基づいたパケットの中継を行う。DHCPサーバ1903は、DHCPプロトコルに基づきユーザ端末にIPアドレスを配布する。認証サーバ1901は、ユーザ認証の結果を状態変更指示パケットとしてLANスイッチ1600に通知する。このネットワークシステムにおいて、各ネットワークに接続された機器には、そのネットワークに属するIPアドレスが割り当てられている(図中IPアドレスと表記されたアドレス)。各ネットワークに接続された各

(11)

特開2002-84306

20

機器のインターフェースには物理アドレス(以下MACアドレスと記載する)が設定されている。以下の説明で必要となるMACアドレスは、図中に「MACアドレス」と表記されている。

【0104】つぎに、ユーザ端末1905がネットワークBの情報コンセント409に接続された場合について説明する。

【0105】図20は、ユーザ端末1905がネットワークBの情報コンセント409に接続された場合の通信シーケンス図である。

【0106】初期状態では、LANスイッチ1600のフィルタリングテーブル1607には、何も登録されていない。また、学習テーブル1606は、MACアドレスフィールド1801にルータ1904のMACアドレス(22:22:00:44:44:44)を、接続ポートフィールド1802にネットワークインターフェースA1602の名前をそれぞれ格納している1つのエントリを持っている。

【0107】まず、ユーザ端末1905は、情報コンセント409に接続されると、DHCPプロトコルによりIPアドレスを要求するためのアドレス要求パケット2001を送信する。この場合、ユーザ端末1905はパケット2001の宛先アドレスをブロードキャストアドレスとして送信する。パケット2001はLANスイッチ1600のネットワークインターフェースB1603により受信され、パケット中継部1601に送られる。

【0108】パケット2001を受信したLANスイッチ1600の中継処理を説明する。

【0109】図21は、パケット受信に対するLANスイッチ1600のパケット中継部1601の中継処理を示すフローチャートである。

【0110】パケット2001を受信するとパケット中継部1601は、パケット2001の宛先アドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先アドレスは学習テーブル1606に登録されていない為、宛先アドレスがブロードキャストアドレスか判断する(処理2102)。宛先アドレスはブロードキャストアドレスである為、受信ポートがアップリンクか判断する(処理2103)。受信ポートはネットワークインターフェースB1603であってアップリンクではない為、パケット2001の送信元アドレスが学習テーブル1606に登録されているか検索する(処理2104)。送信元アドレスであるユーザ端末1905のMACアドレス(22:22:FF:00:00:01)は学習テーブル1606に登録されていない。また、フィルタリングテーブル1607にもこの送信元アドレスは登録されていない為、パケット中継部1601はユーザ端末1905のMACアドレス(22:22:FF:00:00:01)をフィルタリングテーブル1607の1つのエントリのMACアドレスフィールド1

21

701に登録する(処理2105)。

【0111】この場合、図17に示すように、フィルタリングテーブル1607のそのエントリのIPアドレスフィールド1702には「未登録」を示す情報、接続ポートフィールド1703にはネットワークインターフェースB1603の名前「B」がそれぞれ登録される。

【0112】そして、パケット中継部1601はパケット2001をアップリンクにのみ中継し、ルータ1904に送る(処理2105)。

【0113】パケット2001はアドレス要求パケットであるので、ルータ1904のBOOTPリレーエージェント機能によってDHCPサーバ1903に中継される。

【0114】図20において、DHCPサーバ1903から送信されたアドレス配布パケット2002は、ルータ1904のBOOTPリレーエージェント機能により、ユーザ端末1905のMACアドレス(22:22:FF:00:00:01)宛に送られる。

【0115】パケット2002はLANスイッチ1600のネットワークインターフェースA1602により受信され、パケット中継部1601に送られる。パケット中継部1601は、図21に示されたフローチャートに従ってパケット2002を中継処理する。パケット中継部1601は、パケット2002の宛先アドレスであるユーザ端末1905のMACアドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先アドレスは学習テーブル1606に登録されていない為、宛先アドレスがブロードキャストアドレスか判断する(処理2102)。宛先アドレスはブロードキャストアドレスではない為、宛先アドレスがフィルタリングテーブル1607に登録されているか検索する(処理2106)。フィルタリングテーブル1607にはユーザ端末1905のMACアドレスが登録されている為、受信ポートがアップリンクか判断する(処理2107)パケット2002の受信ポートはネットワークインターフェースA1602であり、アップリンクである為、パケット2002の通信プロトコルがIPプロトコルか判断する(処理2108)。通信プロトコルはIPプロトコルである為、パケット2002に含まれる送信元IPアドレスがリレーエージェント(ルータ1904)または認証サーバのIPアドレスか判断する(処理2109)。

送信元IPアドレスはリレーエージェント(ルータ1904)のIPアドレスである為、パケット中継部1601はパケット2002を中継する。この場合、パケット中継部1601はパケット2002の宛先アドレスがMACアドレスフィールド1701の内容と一致するフィルタリングテーブル1607のエントリ#1を参照する。エントリ#1の接続ポートフィールド1703にはネットワークインターフェースB1603の名前が登録されている為、パケット中継部1601は、パケッ

(12)

特開2002-84306

22

ト2002をネットワークインターフェースB1603に中継し、ネットワークインターフェースB1603から送信させる(処理2110)。これによって、ユーザ端末1905にアドレス配布パケット2002が送られる。ここで、ユーザ端末1905に、DHCPサーバ1903から配布されたIPアドレスが「192.168.5.1」であるとする。

【0116】次に、ユーザ端末1905が認証サーバによる認証を受けずにファイルサーバ1902にアクセスを試みる場合について説明する。但し、アクセスのためのプロトコルとしてはIPが用いられる。

【0117】図19に示されたネットワークシステムにおいて、ファイルサーバ1902(IPアドレス192.168.1.2)とユーザ端末1905(IPアドレス192.168.5.1)は、それぞれが接続しているサブネットが異なる。その為、ユーザ端末1905がファイルサーバ1902にアクセスするために送信するパケット2003は、宛先IPアドレスとしてファイルサーバ1902のIPアドレス(192.168.

1.2)を含み、宛先MACアドレスとしてルータ1904のMACアドレス(22:22:00:44:44:44)を含む。パケット2003はユーザ端末1905から送信され、LANスイッチ1600のネットワークインターフェースB1603に受信される。ネットワークインターフェースBは受信したパケット2003をパケット中継部1601に送る。

【0118】パケット2003を受信したLANスイッチ1600のパケット中継部1601の処理を図21に示されたフローチャートを用いて説明する。

【0119】パケット2003を受信するとパケット中継部1601は、パケット2003の宛先MACアドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先MACアドレスであるルータ1904のMACアドレスは学習テーブル1606に登録されている。従って、パケット中継部1601は、パケット2003の通信プロトコルがIPプロトコルであるか、また、パケット2003に含まれる送信元MACアドレスがフィルタリングテーブル1607に登録されているかを確認する(処理2111)。パケット2003の通信プロトコルはIPプロトコルであり、また、送信元MACアドレスであるユーザ端末1905のMACアドレスはフィルタリングテーブル1607に登録されている。従って、パケット中継部1601は、フィルタリングテーブル1607のうちのユーザ端末1905のMACアドレスが登録されているエントリにおけるIPアドレスフィールド1702に、パケット2003に含まれる送信元IPアドレスを登録する(処理2111)。この場合、図17に示されるように、フィルタリングテーブル1607のうちのユーザ端末1905のMACアドレスが登録されているエントリにおけるIPアドレス

(13)

特開2002-84306

23

フィールド1702には「未登録」を示す情報が元々登録されている為、その情報がパケット2003に含まれる送信元IPアドレスに変更されることになる。尚、パケット2003に含まれる送信元IPアドレスは、DHCPサーバ1903からユーザ端末1905に配布されたIPアドレス(192.168.5.1)である。

【0120】その後、パケット中継部1601は、学習テーブル1606のうちの宛先MACアドレスが登録されたエントリにおける接続ポートフィールド1802の内容に従って、パケット2003をアップリンクに中継する。パケット2003はアップリンクからルータ1904に送られる。パケット2003はIPプロトコルの仕様に基づいてルータ1904によってファイルサーバ1902に中継される。

【0121】ファイルサーバ1902は、パケット2003を受信すると、ユーザ端末1905によって要求されたデータを含むパケット2004を、応答パケットとして送信する。パケット2004はルータ1904に受信され、中継されてLANスイッチ1600に送られる。LANスイッチ1600のネットワークインターフェースA1602はパケット2004を受信し、パケット中継部1601に送る。

【0122】次に、パケット2004を受信したLANスイッチ1600のパケット中継部1601の処理について図21に示されたフローチャートに従って説明する。

【0123】まず、パケット2004は宛先MACアドレスとしてユーザ端末1905のMACアドレス(22:22:FF:00:00:01)、宛先IPアドレスとしてユーザ端末1905のIPアドレス(192.168.5.1)、送信元IPアドレスとしてファイルサーバ1902のIPアドレス(192.168.1.2)を含む。

【0124】パケット中継部1601は、パケット2004の宛先MACアドレスであるユーザ端末1905のMACアドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先MACアドレスは学習テーブル1606に登録されていない為、宛先MACアドレスがブロードキャストアドレスか判断する(処理2102)。宛先MACアドレスはブロードキャストアドレスではない為、宛先MACアドレスがフィルタリングテーブル1607に登録されているか検索する(処理2106)。フィルタリングテーブル1607にはユーザ端末1905のMACアドレスが登録されている為、受信ポートがアップリンクか判断する(処理2107)パケット2004の受信ポートはネットワークインターフェースA1602であり、アップリンクである為、パケット2004の通信プロトコルがIPプロトコルか判断する(処理2108)。通信プロトコルはIPプロトコルである為、パケット2004に含まれる送信

24

元IPアドレスがリレーエージェント(ルータ1904)または認証サーバのIPアドレスか判断する(処理2109)。送信元IPアドレスはファイルサーバ1902のIPアドレスである為、パケット2004を廃棄する(処理2109)。即ち、パケット2004はLANスイッチ1600からユーザ端末1905に送信されない。従って、ユーザ端末1905からファイルサーバ1902へのアクセスは成立しない。

【0125】次に、ユーザ端末1905が認証サーバ1901から認証を受ける場合について説明する。

【0126】ユーザは、認証サーバ1901による認証を受ける為、ユーザ端末1905にユーザID及びパスワードを入力する。ユーザ端末1905は、入力されたユーザIDとパスワードを含むパケット2005を認証サーバ1901宛に送信する。この場合において、認証サーバ(IPアドレス192.168.1.1)とユーザ端末1905(IPアドレス192.168.5.1)のそれぞれが属するサブネットは異なる。その為、パケット2005は、宛先IPアドレスとして認証サーバ1901のIPアドレス(192.168.1.1)を含み、宛先MACアドレスとしてルータ1904のMACアドレス(22:22:00:44:44:44)を含む。パケット2005はユーザ端末1905から送信され、LANスイッチ1600のネットワークインターフェースB1603に受信される。ネットワークインターフェースBは受信したパケット2005をパケット中継部1601に送る。

【0127】パケット2005を受信したLANスイッチ1600のパケット中継部1601の処理を図21に示されたフローチャートを用いて説明する。

【0128】パケット2005を受信するとパケット中継部1601は、パケット2005の宛先MACアドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先MACアドレスであるルータ1904のMACアドレスは学習テーブル1606に登録されている。従って、パケット中継部1601は、パケット2005の通信プロトコルがIPプロトコルであるか、また、パケット2005に含まれる送信元MACアドレスがフィルタリングテーブル1607に登録されているかを確認する(処理2111)。パケット2005の通信プロトコルはIPプロトコルであり、また、送信元MACアドレスであるユーザ端末1905のMACアドレスはフィルタリングテーブル1607に登録されている。更に、パケット2005に含まれる送信元IPアドレスもフィルタリングテーブル1607に登録されている。従って、パケット中継部1601は、学習テーブル1606のうちの宛先MACアドレスが登録されたエントリにおける接続ポートフィールド1802の内容に従って、パケット2005をアップリンクに中継する。パケット2005はアップリンクからルータ1904に



25

送られる。パケット2005はIPプロトコルの仕様に基づいてルータ1904によって認証サーバ1901に中継される。

【0129】認証サーバ1901は、ユーザ端末1905から送られたパケット2005に含まれるユーザIDとパスワードが、ネットワークの使用を許可されたユーザのものであった場合、状態変更指示通知パケット2006をLANスイッチ1600の状態変更指示通知パケット処理部1608宛に送信する。この状態変更指示通知パケット2006は、ユーザ端末1905のIPアドレス(192.168.5.1)と「許可」を示す情報を含む。状態変更指示通知パケット2006は、ルータ1904によってLANスイッチ1600に中継される。LANスイッチ1600のネットワークインターフェースA1602は状態変更指示通知パケット2006を受信し、パケット中継部1601を介して状態変更指示通知パケット処理部1608に送る。状態変更指示通知パケット処理部1608は、状態変更指示通知パケット2006を受けて、状態変更指示通知パケット2006に含まれるIPアドレス(192.168.5.1)をフィルタリングテーブル1607から検索する。状態変更指示通知パケット処理部1608は、フィルタリングテーブル1607からIPアドレス(192.168.5.1)が登録されているエントリを見つけ、そのエントリのMACアドレスフィールド1701と接続ポートフィールド1703から、MACアドレス(22:22:FF:00:00:01)と接続ポートの名前(B)を読み出す。状態変更指示通知パケット処理部1608は、読み出したMACアドレスと接続ポートの名前が登録された新たなエントリを学習テーブル1606に追加する。

【0130】図22は、学習テーブル1606の構成図(2)である。図22に示されるように、学習テーブル22は、#2のエントリとしてMACアドレス(22:22:FF:00:00:01)と接続ポートの名前(B)を含むエントリを持つ。

【0131】認証サーバ1901の認証後、ユーザ端末1905が再度ファイルサーバ1902にアクセスする為にパケット2007を送信すると、上述と同様に、パケット2007は、LANスイッチ1602及びルータ1904によって中継されてファイルサーバ1902に送られる。

【0132】ファイルサーバ1902は、パケット2007を受信すると、ユーザ端末1905によって要求されたデータを含むパケット2008を、応答パケットとして送信する。パケット2008はルータ1904に受信され、中継されてLANスイッチ1600に送られる。LANスイッチ1600のネットワークインターフェースA1602はパケット2008を受信し、パケット中継部1601に送る。パケット2008を受信した

(14)

特開2002-84306

26

パケット中継部1601は、図21に示されたフローチャートに従って次のように処理する。

【0133】パケット2008は宛先MACアドレスとしてユーザ端末1905のMACアドレス(22:22:FF:00:00:01)、宛先IPアドレスとしてユーザ端末1905のIPアドレス(192.168.5.1)、送信元IPアドレスとしてファイルサーバ1902のIPアドレス(192.168.1.2)を含む。

【0134】パケット中継部1601は、パケット2008の宛先MACアドレスであるユーザ端末1905のMACアドレスが学習テーブル1606に登録されているか検索する(処理2101)。宛先MACアドレスはユーザ端末1905のMACアドレス(22:22:FF:00:00:01)であるので、図22に示されるように学習テーブル1606に登録されている。従って、パケット中継部1601は、パケット2008の通信プロトコルがIPプロトコルであるか、また、パケット2008に含まれる送信元MACアドレスがフィルタリングテーブル1607に登録されているかを確認する(処理2111)。パケット2008の通信プロトコルはIPプロトコルであり、また、送信元MACアドレスであるルータ1904のMACアドレスはフィルタリングテーブル1607に登録されていない為、フィルタリングテーブル1607には何も登録しない。そして、パケット中継部1601は、学習テーブル1606のうちの宛先MACアドレスが登録されたエントリにおける接続ポートフィールド1802の内容に従って、パケット2008をネットワークインターフェースB1603に中継する。パケット2008はネットワークインターフェースB1603からユーザ端末1905に送られる。これにより、ユーザ端末1905からファイルサーバ1902へのアクセスが成立する。

【0135】認証を受けた後、ユーザ端末1905が一定時間ファイルサーバと通信をしなかった場合、学習テーブル1606のエントリ(エントリ#2)は自動的に削除される。従って、再びユーザ端末1905が認証サーバによる認証を受けるまではファイルサーバ1902へのアクセスはできなくなる。また、DHCPサーバ1903によるアドレス配布において、通常、配布されたアドレスの使用期限が設けられている。このため、DHCPサーバ1903は、ユーザ端末1905にアドレス配布を行ってから所定の時間が経過し、アドレスの使用期限が過ぎたら、タイムアウト通知2009を認証サーバ1901に対して行う。タイムアウト通知2009を受けた認証サーバは、使用期限の過ぎたIPアドレス(この場合192.168.5.1)、および「禁止」という情報を含む状態変更指示通知パケット2010をLANスイッチ1600の状態変更指示通知パケット処理部1608宛に送信する。状態変更指示通知パケット



27

2010は、ルータ1904によってLANスイッチ1600に中継される。LANスイッチ1600のネットワークインターフェースA1602は状態変更指示通知パケット2010を受信し、パケット中継部1601を介して状態変更指示通知パケット処理部1608に送る。状態変更指示通知パケット処理部1608は、状態変更指示通知パケット2010を受けて、状態変更指示通知パケット2010に含まれるIPアドレス(192.168.5.1)をフィルタリングテーブル1607から検索する。状態変更指示通知パケット処理部1608は、フィルタリングテーブル1607からIPアドレス(192.168.5.1)が登録されているエントリを見つけ、そのエントリのMACアドレスフィールド1701から、MACアドレス(22:22:FF:00:00:01)を読み出す。状態変更指示通知パケット処理部1608は、更に、読み出したMACアドレスを学習テーブル1606から検索し、そのMACアドレスが登録されているエントリを見つける。状態変更指示通知パケット処理部1608は、フィルタリングテーブル1607と学習テーブル1606の双方から、見つけたエントリをそれぞれ削除する。その結果、ユーザ端末1905は、再び認証を受けない限りファイルサーバ1902にアクセスできなくなる。

【0136】以上のように、LANスイッチ1600を用いることで、認証を受けていないユーザ端末1905からのファイルサーバ1902へのアクセスが防止され、認証を受けたユーザ端末1905からのファイルサーバ1902へのアクセスが許可されるネットワークシステムを構築できる。また、情報コンセントに接続されたユーザ端末が一定時間無通信である場合や、ユーザ端末に配布されたアドレスの使用期限が過ぎた場合に、LANスイッチ1600内のテーブルを自動的に変更し、再びユーザ端末が認証を受けるまではファイルサーバ1902へのアクセスを防止することもできる。

【0137】図23は、パケット通信装置としてルータ2300を用いたネットワークシステムの構成図である。

【0138】ルータ2300は、例えば、複数のネットワークインターフェースA2302~D2305、パケット中継部2301、IPアドレス登録表2306を備える。

【0139】パケット中継部2301は、IPプロトコルに基づいてパケット中継を行う。また、パケット中継部2301はIPアドレス登録表2306に登録されていないIPアドレスを持つユーザ端末からのパケットに対して、カプセル化処理を行う。ネットワークインターフェースA2302~D2305は、それぞれ異なるネットワークに接続され、パケットの送受信を行う。IPアドレス登録表2306には、認証を受けたユーザ端末のIPアドレスが登録される。

(15)

特開2002-84306

28

【0140】また、このネットワークシステムは、例えば、ルータ2300と、ルータ2300のネットワークインターフェースA2302に、ネットワークAを介して接続された認証サーバ2310及びファイルサーバ2311と、ネットワークインターフェースB2303~D2305に、ネットワークB~Dをそれぞれ介して接続され、ユーザが端末を自由に接続できる複数の情報コンセント409と、情報コンセント409を介してネットワークB2313に接続されたユーザ端末2312とを含む。認証サーバ2310は、ユーザ認証を行うと共に、その結果をルータ2300に通知し、後述するカプセル化されたパケットの送受信を行う。

【0141】つぎに、このネットワークシステムにおいて、ユーザ端末2312がネットワークB2313に接続された情報コンセント409に接続された場合について説明する。

【0142】図27は、初期状態でのIPアドレス登録表2306の構成図である。図24は、ユーザによってユーザ端末2312が情報コンセント409に接続された場合の通信シーケンス図である。

【0143】ユーザ端末2312が認証サーバ2310による認証を受けずにファイルサーバ2311へのアクセスを試みた場合について説明する。

【0144】認証を受けていないユーザ端末2312は、ファイルサーバ2311にアクセスするため、ファイルサーバ2311のIPアドレス(192.168.10.2)宛のパケット2400を送信する。この場合、パケット2400は、ルータ2300のネットワークインターフェースB2303に受信され、パケット中継部2301に送られる。パケット中継部2301は、ユーザ端末2312からのパケット2400を受信し、中継処理を行う。

【0145】図25は、ルータ2300のパケット中継装置2301の中継処理を示すフローチャートである。

【0146】パケット2400を受信すると、パケット中継部2301は、パケット2400の宛先アドレスがルータ2300のカプセル化用アドレスか判断する(処理2501)。パケット2400の宛先アドレスは、ファイルサーバ2311のIPアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット2400の送信元アドレスがIPアドレス登録表2306に登録されているか検索する(処理2502)。送信元アドレスであるユーザ端末2312のIPアドレスはIPアドレス登録表2306に登録されていない為、パケット中継部2301は、パケット2400をカプセル化する(処理2503)。

【0147】ここで、「カプセル化」とは、IPヘッダを含むパケット2400全体を1つのデータとみなし、このデータに対して、宛先アドレスとして認証サーバ2310のカプセル化用アドレス(192.168.10

29

0. 100)、送信元アドレスとしてルータ2300のカプセル化用アドレス(192. 168. 100. 101)を含むIPヘッダを付加することにより、新たなパケット(カプセル化したパケット)を作成することである。この為、カプセル化したパケットは、元々の宛先アドレス(例えば、ファイルサーバ2311のIPアドレス)に係わらず、認証サーバ2310に送信されることになる(処理2504)。

【0148】ここで、カプセル化されたパケットを受信した認証サーバ2310の処理について説明する。

【0149】図26は、パケットを受信した認証サーバ2310の処理を示すフローチャートである。

【0150】カプセル化されたパケットを受信した認証サーバ2310は、パケットの宛先アドレスが認証サーバのカプセル化用アドレスか判断する(処理2601)。

カプセル化されたパケットの宛先アドレスは認証サーバのカプセル化アドレスである為、パケットの送信元アドレスがルータ2300のカプセル化用アドレスであるか判断する(処理2602)。送信元アドレスはルータのカプセル化用アドレスである為、受信したパケットのカプセル化を解除し、元々のパケット2400を復元する(処理2603)。カプセル化を解除するとは、カプセル化されたパケットからIPヘッダを取り除き、カプセル化されたパケットにデータとして含まれていたカプセル化される前のパケット2400を取り出すことである。

【0151】次に、認証サーバ2310は、カプセル化を解除したパケット2400の宛先アドレスが認証サーバのIPアドレスであるか判断する(処理2604)。パケット2400の宛先アドレスはファイルサーバ2311のIPアドレスであって、認証サーバ2310のIPアドレスではない。従って、認証サーバ2310はパケット2400を廃棄する。

【0152】この結果、認証を受けていないユーザ端末2312は、ファイルサーバ2311へアクセスすることはできない。

【0153】次に、ユーザ端末2312が認証サーバ2310から認証を受ける場合について図24及び図25を用いて説明する。

【0154】ユーザは、認証サーバ2310による認証を受ける為、ユーザ端末2312にユーザID及びパスワードを入力する。ユーザ端末2312は、入力されたユーザIDとパスワードを含むパケット2401を認証サーバ2310宛に送信する。パケット2401はルータ2300のネットワークインターフェースB2303に受信される。ネットワークインターフェースB2303は受信したパケット2401をパケット中継部2301に送る。

【0155】パケット2401を受信したルータ2300のパケット中継部2301の処理を図25に示された

(16)

特開2002-84306

30

フローチャートを用いて説明する。

【0156】パケット2401を受信すると、パケット中継部2301は、パケット2401の宛先アドレスがルータ2300のカプセル化用アドレスか判断する(処理2501)。パケット2401の宛先アドレスは、認証サーバ2310のIPアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット2401の送信元アドレスがIPアドレス登録表2306に登録されているか検索する(処理2502)。送信元アドレスであるユーザ端末2312のIPアドレスはIPアドレス登録表2306に登録されていない為、パケット中継部2301は、パケット2401をカプセル化する(処理2503)。そしてパケット中継部2301は、カプセル化したパケットを認証サーバ2310に送信する(処理2504)。

【0157】図26に示されるように、認証サーバ2310は、カプセル化されたパケットを受信すると、パケットの宛先アドレスが認証サーバのカプセル化用アドレスか判断する(処理2601)。カプセル化されたパケットの宛先アドレスは認証サーバのカプセル化用アドレスである為、パケットの送信元アドレスがルータ2300のカプセル化用アドレスであるか判断する(処理2602)。送信元アドレスはルータのカプセル化用アドレスである為、受信したパケットのカプセル化を解除し、元々のパケット2401を取り出す(処理2603)。次に、認証サーバ2310は、カプセル化を解除したパケット2401の宛先アドレスが認証サーバのIPアドレスであるか判断する(処理2604)。パケット2401の宛先アドレスは認証サーバ2310のIPアドレスである為、認証を行う(処理2605)。認証の処理において、認証サーバ2310は、パケット2401に含まれるユーザIDとパスワードがネットワークの使用許可を与えられたユーザのものとも一致するか比較し、一致したら、ユーザ端末2312の認証が成功したことを通知するパケット2402を生成し、更にこのパケット2402をカプセル化して送信する(処理2606)。パケット2402は宛先アドレスとしてユーザ端末2312のIPアドレスを含むIPヘッダを持つ。認証サーバ2310によるカプセル化は、宛先アドレスとしてルータ2300のカプセル化用アドレス(192. 168. 100. 101)、送信元アドレスとして認証サーバ2310のカプセル化用アドレス(192. 168. 100. 100)を含むIPヘッダを、パケット2402に付加し、新たなパケット(カプセル化したパケット)を作成することである。従って、カプセル化されたパケットはルータ2300に送信される。

【0158】カプセル化されたパケットはネットワークインターフェースA2302により受信され、パケット中継部2301に送られる。図25に示されたフローチャートに従って、パケット中継部2301は、受信した

31

パケットの宛先アドレスがルータのカプセル化用アドレスか判断する(処理2501)。宛先アドレスはルータ2300のカプセル化用アドレスである為、送信元アドレスが認証サーバ2310のカプセル化用アドレスであるか判断する(処理2505)。送信元アドレスは認証サーバ2310のカプセル化用アドレスである為、パケット中継部2301は、受信したパケットのカプセル化を解除し、元々のパケット2402を取り出す(処理2506)。そして、パケット中継部2301は、パケット2402を中継し(処理2507)、ユーザ端末2312へ送信する。

【0159】また、ユーザ端末2312の認証が成功すると、認証サーバ2310は、ルータ2300に対して、ユーザ端末2312のIPアドレス(192.168.3.3)をIPアドレス登録表2306へ登録するよう指示するパケット2403を送信する。

【0160】パケット2403はネットワークインターフェースA2302により受信され、パケット中継部2301に送られる。パケット中継部2301は、パケット2403を受け取ると、パケット2403による指示に従って、IPアドレス登録表2306にユーザ端末2312のIPアドレス(192.168.3.3)を登録する。

【0161】その後、ユーザ端末2312がファイルサーバ2311にアクセスする場合について説明する。

【0162】ユーザ端末2312は、ファイルサーバ2311にアクセスするため、ファイルサーバ2311のIPアドレス(192.168.10.2)宛のパケット2404を送信する。パケット2404は、ルータ2300のネットワークインターフェースB2303に受信され、パケット中継部2301に送られる。

【0163】図25に示されるように、パケット2404を受信すると、パケット中継部2301は、パケット2404の宛先アドレスがルータ2300のカプセル化用アドレスか判断する(処理2501)。パケット2404の宛先アドレスは、ファイルサーバ2311のIPアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット2404の送信元アドレスがIPアドレス登録表2306に登録されているか検索する

(処理2502)。送信元アドレスであるユーザ端末2312のIPアドレスはIPアドレス登録表2306に登録されている為、ルータ中継部2301はパケット2404を中継し(処理2508)、パケット2404をファイルサーバ2311へ送信する。

【0164】ファイルサーバ2311は、パケット2404を受信すると、ユーザ端末2312によって要求されたデータを含むパケット2405を応答パケットとして送信する。パケット2405は、ネットワークインターフェースA2302により受信され、パケット中継部2301に送られる。パケット中継部2301は、パケ

(17)

特開2002-84306

32

ット2405の宛先アドレスがルータ2300のカプセル化用アドレスか判断する(処理2501)。パケット2405の宛先アドレスは、ユーザ端末2312のIPアドレスであり、ルータのカプセル化用アドレスではない。そこで、パケット2405の送信元アドレスがIPアドレス登録表2306に登録されているか検索する

(処理2502)。送信元アドレスであるファイルサーバ2311のアドレス(192.168.10.2)はIPアドレス登録表2306に登録されている。そこで、ルータ中継部2301はパケット2405を中継し(処理2508)、パケット2405をユーザ端末2312に送信する。このように、ユーザ端末2312が認証サーバ2310による認証を受けた後は、ユーザ端末2312からファイルサーバ2311へのアクセスが可能となる。

【0165】認証サーバ2310は、ユーザ端末2312の認証が成功した後、定期的にユーザ端末2312に対してICMP(Internet Control Message Protocol)に従ったICMPエコーリクエスト2406を送信し、ICMPエコーリクエスト2406に対する応答データであるICMPエコーリプライ2407がユーザ端末2312から返送されてくることを確認する。

【0166】ICMPエコーリクエスト2406を送信してから一定時間以内にユーザ端末2312からICMPエコーリプライ2407が送られてこない場合、認証サーバ2310は、ユーザ端末2312のIPアドレス(192.168.3.3)をIPアドレス登録表から削除するよう指示するパケットをルータ2300に送信する。そのパケットはネットワークインターフェースA2302により受信され、パケット中継部2301に送られる。パケット中継部2301は、そのパケットを受け取ると、パケットによる指示に従って、IPアドレス登録表2306からユーザ端末2312のIPアドレス(192.168.3.3)を削除する。その結果、ユーザ端末2312が再び認証を受けるまでは、ユーザ端末2312からファイルサーバ2311へのアクセスはできなくなる。

【0167】以上のように、ルータ2300を用いることで、認証を受けていないユーザ端末2312からファイルサーバ2311へのアクセスが防止され、認証を受けたユーザ端末2312からファイルサーバ2311へのアクセスが許可されるネットワークシステムを構築することができる。また、認証サーバ2310が定期的にユーザ端末2311からのICMPエコーリプライ2407の受信を確認することにより、ユーザ端末2311がネットワークから離脱したり、ネットワークの使用を中止した場合、ユーザ端末2311のIPアドレスをIPアドレス登録表2306から自動的に削除し、ユーザ端末2311によるファイルサーバ2311へのアクセスを防止することができる。



【0168】図28は、複数のパケット通信装置A～C 2801とルータ2820によって複数のネットワークが接続されたネットワークシステムの構成図である。

【0169】このネットワークシステムは、例えば、パケット通信装置A～C 2801と、各パケット通信装置A～C 2801と接続されたルータ2820と、それぞれネットワーク（IPサブネット）を介してルータ2820に接続されたサーバA～C 2803、フィルタリング状態管理装置2802、DHCPサーバ2807と、各パケット通信装置A～C 2801と接続された1つ以上のネットワーク（IPサブネット）を含む情報コンセントシステム2830と、情報コンセントシステム2830のうちの任意のネットワークに接続される1台以上のユーザ端末2806とを含む。各パケット通信装置A～C 2801は、アドレス学習テーブル2811と、対象外アドレステーブル2812と、認証用アドレステーブル2813とを備え、情報コンセントシステム2830に接続されたユーザ端末2806から送られてくるパケットの中継またはフィルタリング（廃棄）を行なう。各パケット通信装置A～C 2801はOSI参照モデルのデータリンク層でパケットの中継を行うLANスイッチである。各パケット通信装置A～C 2801は、DHCPリレーエージェント機能を有し、接続された各IPサブネットに対応するIPアドレスを持つものとする。

【0170】各サーバA～C 2803は、それぞれユーザ認証部2804と認証状態検出部2805を備える。ユーザ認証部2804はユーザを識別する為の情報を蓄積するユーザアカウント2840を備える。認証状態検出部2805はサブネットテーブル2814を備える。ユーザ認証部2804は各サーバA～C 2803（パーソナルコンピュータ）により実行されるソフトウェアとして実現されている。ユーザ認証部2804としては、OS (Operating System)の持つログイン機能が用いられるが、その他の認証方法、例えばユーザにパスワードを入力させるWWW(World Wide Web)のページ等が用いられても構わない。また、複数のユーザ認証部2804がネットワークシステムに存在する場合、その全てが同じ方式のユーザ認証を行ってもよいし、それぞれが異なる方式のユーザ認証を行ってもよい。認証状態検出部2805も、各サーバA～C 2803により実行されるソフトウェアとして実現されている。ユーザ認証部2804により認証（ログイン）が行われた場合、ユーザ認証部2804は同じサーバ2803において動作する認証状態検出部2805に対して、認証（ログイン）に成功したユーザ端末のIPアドレスを通知する。

【0171】フィルタリング状態管理装置2802はサブネットテーブル2814を備える。フィルタリング状態管理装置2802は、各サーバA～C 2803の認証状態検出部2805およびパケット通信装置2801とネットワークを介して通信する。

【0172】このネットワークシステムにおいて、ユーザは自由にユーザ端末（ノートパソコン等）を情報コンセントシステム2830における1つ以上のネットワーク（IPサブネット147. 3. 1. 0から147. 5. 3. 0）の何れかに接続することができ、ネットワークシステムを利用することができる。

【0173】このネットワークシステムにおいて、通信は全てIPプロトコル（IPv4）に従って行われる。尚、その他の通信プロトコル（例えばIPv6）が用いられるネットワークシステムであっても構わない。各ネットワーク（IPサブネット）にはIPサブネット番号が割り当てられている。尚、サブネットマスクは全て24ビット長であるとする。各ネットワークに接続された機器には、そのネットワークに属するIPアドレスが割り当てられている。図28においてIPと記されている。各ネットワークは全てIEEEで規定されているCSMA/CD型の802. 3ネットワークである。尚、各ネットワークは、その他のネットワークであっても構わない。各ネットワークに接続された各機器のインターフェースには物理アドレス（以下、MACアドレスと記載する）が設定されている。以下の説明で必要となるMACアドレスは、図28においてMACと記載されている。

【0174】情報コンセントシステム2830にユーザ端末2806が全く接続されていない初期の状態における各装置の設定について説明する。

【0175】ユーザ認証部2804には、ネットワークの使用が許可されたユーザのユーザIDとパスワードとが登録されている。ユーザ認証部2804としてOSのユーザ認証（ログイン）機能が用いられるので、OSにおけるユーザアカウント2840がこの登録情報に該当する。認証状態検出部2805およびフィルタリング状態管理装置2802にはサブネットテーブル2814が設定されている。

【0176】図29はサブネットテーブル2814の構成図である。

【0177】サブネットテーブル2814の各エントリは、サブネットアドレスフィールド2901、サブネットマスクフィールド2902、フィルタリング状態管理装置のIPアドレスフィールド2903、パケット通信装置のIPアドレスフィールド2904からなる。パケット通信装置のIPアドレスフィールド2904には、サブネットアドレスフィールド2901およびサブネットマスクフィールド2902に登録されたサブネットアドレス及びサブネットマスクを論理積したアドレスを持つIPサブネットが接続されているパケット通信装置2801のIPアドレスが登録される。IPアドレスフィールド2904に登録されたIPアドレスを持つパケット通信装置2801に指示を出すフィルタリング状態管理装置2802のIPアドレスがフィルタリング状態管



理装置のIPアドレスフィールド2903に登録される。ネットワークシステム内のフィルタリング状態管理装置2802は1つだけなので、サブネットテーブル2814の全エントリのフィルタリング状態管理装置のIPアドレスフィールド2903には、同じIPアドレスが登録されている。尚、ネットワークシステム内に複数のフィルタリング状態管理装置2802を設けて、サブネットテーブル2814のエントリごとに異なるIPアドレスを登録し、フィルタリング状態管理装置2802の処理を分散させることも可能である。認証状態検出部2805は、ユーザによるログインを検出すると、ユーザの使用するユーザ端末2806のIPアドレスが属するIPサブネットをサブネットテーブル2814で検索し、該当するエントリの内容からユーザのログインを通知すべきフィルタリング状態管理装置2802を決定する。同様に、フィルタリング状態管理装置2802はサブネットテーブル2814の内容からログインしたユーザ端末のIPアドレスを通知すべきパケット通信装置2801を決定する。

【0178】各パケット通信装置A~C2801が備えるアドレス学習テーブル2811には、初期状態では1つもエントリが登録されていない。アドレス学習テーブル2811の内容については後述する。

【0179】図30は認証用アドレステーブル2813の構成図である。

【0180】認証用アドレステーブル2813には、ユーザ認証部2804を備えるサーバ2803のIPアドレスと、その他にユーザ認証に必要となる機能（例えばDNS（Domain Name System））を提供する機器のIPアドレスが登録される。図30に示された認証用アドレステーブル2813には、各サーバA~C2803のIPアドレスが登録されている。また、認証用アドレステーブル2813は、ユーザ認証を受けていないユーザにも公開してよい情報を持つサーバのIPアドレスを登録する為に利用されても良い。

【0181】図31はパケット通信装置A2801の対象外アドレステーブル2812の構成図である。

【0182】対象外アドレステーブル2812には、ユーザが認証を受けなくてもアクセスしてよい情報機器のMACアドレスが登録される。対象外アドレステーブル2812に登録されるべき情報機器は、ルータ等のパケット通信装置、プリンタ等の自発的にユーザ認証（ログイン）を行えない機器などである。これらの機器のMACアドレスが、その機器と同じネットワークに接続されているパケット通信装置2801の対象外アドレステーブル2812に登録される。図31に示された対象外アドレステーブル2812には、ルータ2820の備えるネットワークインターフェースのうち、パケット通信装置A2801と接続されているネットワークインターフェースのMACアドレスが登録されている。

【0183】上述した初期状態で、情報コンセントシステム2830にユーザ端末2806が接続された場合、ユーザ端末2806は、DHCPサーバ2807に対する通信、ルータ2820に対するARP（Address Resolution Protocol）通信、およびユーザ認証部2804との通信だけが許可される。その他の通信はパケット通信装置A2801によりフィルタリングされる。フィルタリングとは、許可されていない通信の為にパケットを廃棄することである。

10 【0184】図28に示されたネットワークシステムにおいて、ユーザによってユーザ端末2806が情報コンセントシステム2830におけるネットワーク（IPサブネット147.3.3.0）に接続され、ユーザ端末2806によりユーザ認証（ログイン）が行われる場合の通信シーケンス図を図33に示す。

【0185】ユーザ端末2806が認証（ログイン）を行うために通信するサーバ2803はサーバAであるとし、サーバAのIPアドレス137.1.1.1はユーザ端末2806またはユーザ端末2806のユーザに既知であるものとする。

【0186】情報コンセントシステム2830のネットワーク（IPサブネット147.3.3.0）にユーザ端末2806が接続された場合、その時点ではユーザ端末2806にはIPアドレスが割り当てられていない。そこで、図28に示されたネットワークシステムにおいては、DHCPを使ってユーザ端末2806にIPアドレスが割り当てられる。尚、DHCP以外の方法によってユーザ端末2806にIPアドレスが割り当てられても構わない。例えば、ユーザ自身によってユーザ端末2806にIPアドレスが設定されても構わない。DHCP以外の方法が用いられる場合、パケット通信装置2801のDHCPリレーエージェント機能は不要である。

【0187】まず、ユーザ端末2806が情報コンセントシステム2830のネットワーク（IPサブネット147.3.3.0）に接続されると、ユーザ端末2806は、DHCPプロトコルによりIPアドレスを要求する為のアドレス要求パケットを送信する。この場合、ユーザ端末2806は、パケットの宛先アドレスをブロードキャストアドレスとしてブロードキャスト送信する。アドレス要求パケットはパケット通信装置A2801により受信される。

【0188】図32は、パケットを受信した各パケット通信装置A~C2801の中継処理を示すフローチャートである。

【0189】パケット通信装置A2801は、ユーザ端末2806からアドレス要求パケットを受信すると、パケットに含まれる送信元MACアドレス（22:22:00:11:11:11）をアドレス学習テーブル2811から検索する（処理3201）。アドレス学習テーブル2811には、初期状態ではエントリが登録されて

(20)

特開2002-84306

37

いない為、パケットの送信元MACアドレスを対象外アドレステーブル2812から検索する(処理3202)。しかし、図31に示されるように、対象外アドレステーブル2812にはルータ2820のMACアドレスしか登録されていない。つまり、ユーザ端末2806からのパケットに含まれる送信元MACアドレスは何れのテーブルにも登録されていない。よって、パケット通信装置A2801は、送信元MACアドレスをアドレス学習テーブル2811の1つのエントリに登録する。

【0190】その後、パケット通信装置A2801は、アドレス要求パケットの宛先IPアドレスを認証用アドレステーブル2813から検索しようと試みる(処理3204)。しかし、アドレス要求パケットの宛先アドレスはブロードキャストアドレスである為、認証用アドレステーブル2813には登録されていない。そこで、パケット通信装置A2801は、受信したパケットがDHCPによるアドレス要求パケットであるか判断する(処理3205)。受信したパケットはアドレス要求パケットである為、パケット通信装置A2801は、DHCPリレーエージェント機能により、アドレス要求パケットをルータ2820を介してDHCPサーバ2807に中継する(処理3208)。

【0191】図33において、DHCPサーバ2807はアドレス要求パケットを受信し、ユーザ端末2806に対してIPアドレスを割り当てる。DHCPサーバ2807は、ユーザ端末2806と接続されたネットワーク(IPサブネット147.3.3.0)に属するIPアドレス(147.3.3.1)をユーザ端末2806に割り当てる。そして、そのIPアドレスをユーザ端末2806に通知する為、アドレス配布パケットを送信する。その際、ユーザ端末2806が接続されたネットワーク(IPサブネット147.3.3.0)におけるデフォルトゲートウェイのアドレスとして、ルータ2820のIPアドレス147.3.3.251もアドレス配布パケットに含めてユーザ端末2806に通知する。ルータ2820のIPアドレス147.3.3.251についてはアドレス配布パケットとは異なるパケットを用いてユーザ端末2806に通知しても構わない。なお、デフォルトゲートウェイのアドレスをユーザ端末2806に設定する方法として、その他の方法(例えばユーザが入力する)を用いても構わない。アドレス配布パケットはルータ2820によりパケット通信装置A2801に中継される。パケット通信装置A2801は、上述と同様に受信パケットを処理し、DHCPリレーエージェント機能により、アドレス配布パケットをユーザ端末のMACアドレス(22:22:00:11:11:11)宛に送る。これにより、ユーザ端末2806にIPアドレス(147.3.3.1)が割り当てられる。

【0192】次に、ユーザ端末2806がサーバA2803のユーザ認証部2804に対して認証(ログイン)

38

を行う場合について説明する。

【0193】ユーザ端末2806は、IPアドレスが割り当てられると、サーバA2803のユーザ認証部に対して認証(ログイン)を試みる。ユーザ端末2806とサーバAは互いに異なるネットワーク(IPサブネット)に属するため、両者はルータ2820を経由して通信することになる。

【0194】図33において、ユーザ端末2806は、DHCPサーバから通知されたデフォルトゲートウェイのIPアドレス147.3.3.251に対応するMACアドレスを得るために、宛先アドレスとしてブロードキャストアドレスを含むARP Requestパケット3301をブロードキャスト送信する。ARP Requestパケット3301には、送信元MACアドレス及び送信元IPアドレスとして、それぞれユーザ端末2806のMACアドレス及びIPアドレスが含まれる。

【0195】ARP Requestパケット3301は、パケット通信装置A2801により受信される。ARP Requestパケット3301を受信すると、パケット通信装置A2801は、まずARP Requestパケット3301に対してARPパケット学習処理を行い、次にARP Requestパケット3301の中継処理を行う。

【0196】図34は、各パケット通信装置A~C2801によるARPパケット学習処理を示すフローチャートである。

【0197】ARPパケット学習処理において、パケット通信装置A2801は、まずARP Requestパケット3301に含まれる送信元MACアドレスを対象外アドレステーブル2812から検索する(処理3401)。図31に示されている通り、対象外アドレステーブル2812にはルータ2820のMACアドレスだけが登録されているので、その送信元MACアドレスが登録されたエントリは対象外アドレステーブル2812にはない。そこで、パケット通信装置A2801は、その送信元MACアドレスをアドレス学習テーブル2811から検索する(処理3402)。初期状態では、パケット通信装置A2801の学習テーブル2811には何も登録されていない。その為、学習テーブル2811にも、その送信元MACアドレスが登録されたエントリは無い。次に、パケット通信装置A2801は、ARP Requestパケット3301に含まれる送信元IPアドレスをアドレス学習テーブル2811から検索する(処理3403)。同様に学習テーブル2811には何も登録されていない為、その送信元IPアドレスが登録されたエントリは学習テーブル2811には無い。よって、パケット通信装置A2801はARPパケット学習処理を終了する。

【0198】その後、パケット通信装置A2801は図

(21)

特開2002-84306

39

40

32に示されたフローチャートに従って、ARP Requestパケット3301の中継処理を行う。即ち、パケット通信装置A2801は、ARP Requestパケット3301に含まれる送信元MACアドレスをアドレス学習テーブル2811から検索する（処理3201）。上述した通り、アドレス学習テーブル2811には何も登録されていないため、パケット通信装置A2801は、その送信元MACアドレスを対象外アドレステーブル2812から検索する（処理3202）。図31に示されるように対象外アドレステーブル2812にはルータ2820のMACアドレスだけが登録されており、その送信元MACアドレスは何れのエン트리にも登録されていない。そこで、パケット通信装置A2801は、その送信元MACアドレスをアドレス学習テーブル2811に登録する（処理3203）。

【0199】図35、図36及び図37はアドレス学習テーブル2811の構成図である。

【0200】アドレス学習テーブル2811の各エント리는、MACアドレスフィールド、IPアドレスフィールド、状態フィールド、有効期間フィールドを備える。各エント리의MACアドレスフィールドには、パケット通信装置2801に接続されたユーザ端末2806のMACアドレスが登録される。IPアドレスフィールドには、同じエントリに登録されたMACアドレスを持つユーザ端末2806に割り当てられたIPアドレスが登録される。ユーザ端末2806のIPアドレスが不明または割り当てられていない場合には「0.0.0.0」が登録される。状態フィールドには、同じエントリに登録されたMACアドレスと一致する送信元MACアドレスを含むパケットを廃棄することを示す情報（フィルタリング ON）、または中継することを示す情報（フィルタリング OFF）が登録される。有効期間フィールドには、そのエントリが有効である残り時間（有効時間）が秒単位で保持されている上述した通り、パケット通信装置A2801は、ARP Requestパケット3301の送信元アドレスであるユーザ端末2806のMACアドレス（22:22:00:11:11:11）をアドレス学習テーブル2811のMACアドレスフィールドに登録し、IPアドレスフィールドに「0.0.0.0」を、状態フィールドに廃棄を示す情報「フィルタリング ON」を、有効期間フィールドに「3600秒」を登録する。この状態におけるアドレス学習テーブルの構成図を図35に示す。

【0201】「3600秒」という時間は、ネットワークに接続されたユーザ端末2806が、IPアドレスの割り当ても受けず認証（ログイン）も行わなかった場合に、アドレス学習テーブル2811からエントリが削除されるまでの時間に相当する。尚、IPアドレスの割り当てや、認証（ログイン）処理にかかる時間より大きい時間であれば、エント리의有効期間「3600秒」とは

異なる任意の時間でもよい。また、エント리의有効期間が、パケット通信装置2801と同じネットワークに接続された装置に備えられるARPキャッシュ内の情報の有効期間より短い期間であると、パケット通信装置2801とその装置とで情報の不一致が起こる可能性がある。そのため、エント리의有効期間は、ARPキャッシュ内の情報の有効期間より長い時間とする。

【0202】次に、パケット通信装置A2801は、ARP Requestパケット3301に含まれる宛先IPアドレスを認証用アドレステーブル2813から検索する（処理3204）。しかし、ARP Requestパケット3301はIPパケットではない為、ARP Requestパケット3301がDHCPパケットであるか判断する（処理3205）。ARP Requestパケット3301がDHCPパケットではない為、ARP Requestパケット3301に含まれる宛先MACアドレスがブロードキャストアドレスか判断する（処理3206）。宛先MACアドレスはブロードキャストアドレスである為、パケット通信装置A2801は、ARP Requestパケット3301をルータ2820にのみ中継する（処理3209）。

【0203】ルータ2820は、ARP Requestパケット3301を受信し、ARP Replyパケット3302を送信する。ARP Replyパケット3302は、送信元MACアドレス及び送信元IPアドレスとして、それぞれルータ2820のMACアドレス（22:22:00:00:00:03）及びIPアドレス（147.3.3.251）を含む。

【0204】パケット通信装置A2801はARP Replyパケット3302を受信し、ARPパケット学習処理と中継処理を以下のように行う。

【0205】ARPパケット学習処理において、パケット通信装置A2801は、まずARP Replyパケット3302に含まれる送信元MACアドレスを対象外アドレステーブル2812から検索する（処理3401）。図31に示されている通り、対象外アドレステーブル2812には、ルータ2820のMACアドレスが登録されている。従って、パケット通信装置A2801は、送信元MACアドレスであるルータ2820のMACアドレスが登録されたエントリを対象外アドレステーブル2812から見つけ、ARPパケット学習処理を終了する。

【0206】次に、パケット通信装置A2801は、図32に示されたフローチャートに従って、ARP Replyパケット3302に含まれる送信元MACアドレスをアドレス学習テーブル2811から検索する（処理3201）。アドレス学習テーブル2811にはルータ2820のMACアドレスは登録されていないため、パケット通信装置A2801は、その送信元MACアドレスを対象外アドレステーブル2812から検索する（処



41

理3202)。対象外アドレステーブル2812には送信元MACアドレスであるルータ2820のMACアドレスが登録されている為、パケット通信装置A2801はARP Replyパケット3302を中継し(処理3211)、ユーザ端末2806に送信する。ユーザ端末2806は、ARP Replyパケット3302を受信し、ルータ2820のMACアドレスを認識する。

【0207】ユーザ端末2806は、認証(ログイン)を行うため、サーバA2803のユーザ認証部2804に対してログイン要求パケット3303を送信する。ログイン要求パケット3303は、宛先IPアドレスとしてサーバA2803のIPアドレス、宛先MACアドレスとしてルータ2820のMACアドレス、送信元MACアドレス及び送信元IPアドレスとして、それぞれユーザ端末2806のMACアドレス及びIPアドレスを含む。パケット通信装置A2801はログイン要求パケット3303を受信し、図32に示されたフローチャートに従って、ログイン要求パケット3303に含まれる送信元MACアドレスをアドレス学習テーブル2811から検索する(処理3201)。アドレス学習テーブル2811にはユーザ端末2806のMACアドレスが既に登録されている。そこで、パケット通信装置A2801は、送信元MACアドレスが登録されているエントリの状態フィールドを参照する。図35に示される通り、状態フィールドは「フィルタリング ON」を示している為、ログイン要求パケット3303に含まれる宛先IPアドレスを認証用アドレステーブル2813から検索する(処理3204)。認証用アドレステーブル2813にはサーバA2803のIPアドレスが登録されている為、パケット通信装置A2801はログイン要求パケット3303に含まれる送信元IPアドレスがアドレス学習テーブル2811に登録されているか参照する。図35に示される通り、アドレス学習テーブル2811のユーザ端末2806のMACアドレスが登録されたエントリにおけるIPアドレスフィールドには「0.0.0.0」が登録されており、ユーザ端末2806のIPアドレスは登録されていない。従って、パケット通信装置A2801は、そのIPアドレスフィールドに、送信元IPアドレスであるユーザ端末2806のIPアドレス(147.3.3.1)を登録する(処理3210)。この場合、パケット通信装置A2801は有効期間フィールドに保持された時間値は変更しない。

【0208】この状態におけるアドレス学習テーブルの構成図を図36に示す。

【0209】そして、パケット通信装置A2801はログイン要求パケット3303を中継し(処理3211)、ルータ2820に送る。ログイン要求パケット3303はルータ2820によりサーバA2803へ中継される。

【0210】サーバA2803がログイン要求パケット

(22)

特開2002-84306

42

3303を受信すると、サーバA2803のユーザ認証部2804は、ユーザ端末2806に対してパスワードの入力を要求するパスワード要求パケット3304を送信する。ルータ2820はパスワード要求パケット3304を中継し、パケット通信装置A2801に送る。この際、ルータ2820は、パスワード要求パケット3304に含まれる送信元MACアドレスをルータ2820のMACアドレスにして送信する。パケット通信装置A2801は、パスワード要求パケット3304を受信する。パケット通信装置A2801は、図32に示されたフローチャートに従って、ARP Replyパケット3302の中継処理と同様にして、パスワード要求パケット3304に含まれる送信元アドレスをアドレス学習テーブル2811及び対象外アドレステーブル2812から検索する(処理3201及び処理3202)。対象外アドレステーブル2812には送信元MACアドレスであるルータ2820のMACアドレスが登録されている為、パケット通信装置A2801はパスワード要求パケット3304を中継し(処理3211)、ユーザ端末2806に送信する。ユーザ端末2806がパスワード要求パケット3304を受信すると、ユーザ端末2806においてユーザに対してパスワードの入力が促される。ユーザは、ユーザ端末2806にパスワードを入力する。ユーザ端末2806は、入力されたパスワードを含むパケット3305を送信する。パケット通信装置A2801は、パケット3305を受信し、ログイン要求パケット3303の中継処理と同様にして、パケット3305に含まれる送信元MACアドレスをアドレス学習テーブル2811から検索し(処理3201)、また、パケット3305に含まれる宛先IPアドレスを認証用アドレステーブル2813から検索する(処理3204)。認証用アドレステーブル2813には宛先IPアドレスであるサーバA2803のIPアドレスが登録されており、また、送信元IPアドレスであるユーザ端末2806のIPアドレスもアドレス学習テーブル2811に登録されている為(処理3210)、パケット通信装置A2801はパケット3305中継し、ルータ2820に送信する。パケット3305はルータ2820によりサーバA2803へ中継される。サーバA2803がパケット3305を受信すると、ユーザ認証部2804はパケット3305に含まれるパスワードと、ユーザアカウント2840ととして保持している正規のパスワードとを比較し、パスワードが正しいか判定する。ユーザ認証部2804によりパケット3305に含まれるパスワードが正しいと判定されると、ユーザ端末2806のログインがユーザ認証部2804により許可される。ユーザ認証部2804は、ユーザ端末2806に対してログイン完了を通知するログイン完了パケット3306を送信し、また、サーバA2803内の認証状態検出部2805に対してユーザ端末2806のIPアドレス



(147. 3. 3. 1) とログインの完了を知らせる。  
【0211】認証状態検出部2805は、サブネットテーブル2814の各エントリのうち、サブネットマスクフィールド2902に保持されたサブネットマスクとユーザ端末2806のIPアドレスを論理積したアドレスが、サブネットアドレスフィールド2901に保持されたサブネットアドレスと一致するようなエントリを検索する。認証状態検出部2805は、該当するエントリを見つけると、そのエントリのフィルタリング状態管理装置のIPアドレスフィールド2903に登録されたIP  
10 アドレス宛に、ユーザ端末2806のIPアドレスを含む接続通知パケット3307を送信する。例えば、図29に示されたサブネットテーブルにおいて、#3のエントリが、ユーザ端末2806と接続されたネットワーク(IPサブネット)のサブネットアドレスを含み、上述のエントリに該当する。従って、#3のエントリから、接続通知パケット3307を送るべきフィルタリング状態管理装置2802のIPアドレスは「137. 2.  
2. 100」であることがわかる。

【0212】接続通知パケット3307はルータ2820によりフィルタリング状態管理装置2802に中継される。フィルタリング状態管理装置2802は、接続通知パケット3307を受け取ると、サブネットテーブル2814のエントリのうち、サブネットマスクフィールド2902に保持されたサブネットマスクと、通知されたユーザ端末2806のIPアドレスを論理積したアドレスが、サブネットアドレスフィールド2901に保持されたサブネットアドレスと一致するようなエントリを検索する。該当するエントリを見つけると、そのエントリのパケット通信装置のIPアドレスフィールド2904に保持されたIPアドレスを認識する。図29に示されたサブネットテーブルにおいては#3のエントリが上述したエントリに該当する為、#3のエントリから、パケット通信装置のIPアドレスは「147. 3. 1. 2  
20 20」(パケット通信装置A2801のIPアドレス)であることがわかる。フィルタリング状態管理装置2802は、認識したIPアドレスを持つパケット通信装置A2801宛に、ユーザ端末2806のIPアドレス(147. 3. 3. 1)を含む接続許可パケット3308を送信する。

【0213】接続許可パケット3308を通知されたパケット通信装置A2801は、通知されたユーザ端末2806のIPアドレス(147. 3. 3. 1)をアドレス学習テーブル2811から検索する。図36に示される通り、ユーザ端末2806のIPアドレスはアドレス学習テーブル2811の1つのエントリに登録されている。その為、パケット通信装置A2801は、そのエントリの状態フィールドに登録されている情報を「フィルタリング ON」から「フィルタリング OFF」へ変更し、また、有効期間フィールドに新たに「300秒」  
50

という時間を設定する。

【0214】この状態におけるアドレス学習テーブルの構成図を図37に示す。

【0215】その後、送信元MACアドレスとしてユーザ端末2806のMACアドレス(22:22:00:11:11:11)を含むパケットを受信すると、パケット通信装置2801は、図32に示されたフローチャートに従って、送信元MACアドレスをアドレス学習テーブル2811から検索する(処理3201)。この場合、アドレス学習テーブル2811のエントリの1つに送信元MACアドレスが登録されており、また、そのエントリの状態フィールドは「フィルタリングOFF」を示している。その為、パケット通信装置A2801は常に受信したパケットを中継する(処理3211)。その結果、ユーザ端末2806から送信されるパケットはパケット通信装置2801によって廃棄されることがない為、ユーザ端末2801は自由に通信を行うことができる。

【0216】次に、ユーザ端末2806がネットワークから離脱した場合のパケット通信装置A2801における検出方法と処理について説明する。

【0217】パケット通信装置A2801は、アドレス学習テーブル2811の各エントリにおける有効期間フィールドの更新処理を一定時間ごとに起動する。例えば、パケット通信装置A2801は30秒毎に有効期間フィールドの更新処理を起動する。起動する周期は、エントリの有効期間をどの程度の精度で保証するかに依存する。

【0218】このアドレス学習テーブルにおける有効期間フィールドの更新処理について図38を用いて説明する。

【0219】図38は、各パケット通信装置A~C2801によるアドレス学習テーブル2811の更新処理を示すフローチャートである。

【0220】パケット通信装置A2801において、アドレス学習テーブル2811の更新処理が起動されると、まず、アドレス学習テーブル2811の各エントリにおける有効期間フィールドに保持されている残り時間(有効時間)から、更新処理の起動間隔である「30  
40 秒」が減算され、有効時間が更新される(処理3801)。減算された結果、有効期間フィールドに保持されている残り時間(更新された有効時間)が60秒(起動間隔の2倍)より大きい値である場合、パケット通信装置A2801はそのエントリに関してそれ以上の処理を行わず、一旦更新処理を終了する。更新された有効時間が0秒より大きく60秒以下の値であるエントリが存在する場合、パケット通信装置A2801は、そのエントリに登録されているIPアドレスを割り当てられているユーザ端末2806のMACアドレスを再確認する為  
50 に、ARP Requestパケットを、そのユーザ端

(24)

特開2002-84306

45

末2806が接続されているIPサブネットに送信する(処理3803)。更新された有効時間が0秒以下であるエントリが存在する場合、パケット通信装置A2801はそのエントリを削除する(処理3804)。これによって、アドレス学習テーブル2811は、そのエントリに登録されていたMACアドレスを持つユーザ端末2806がネットワークに接続される前の状態に戻る。

【0221】以上の更新処理を実行することにより、パケット通信装置A2801は、定期的(上述した更新処理においては約4分毎)にARP Requestパケットを送信し、ユーザ端末2806の存在を確認する。ユーザ端末2806がネットワークに接続されていれば、ARP Requestパケットに応じてARPreplyパケットがユーザ端末2806から送信される。従って、ARP Requestパケットに対する応答がなければパケット通信装置A2801は、ユーザ端末2806がネットワークから離脱したと解釈し、更新された有効時間が0秒以下になった時点でそのエントリを削除する。

【0222】パケット通信装置A2801における更新処理の起動間隔が30秒であり、パケット通信装置A2801がARP Requestパケットを送信する条件は更新した有効時間が60秒以下(起動間隔の2倍)となることであるから、1つのエントリが削除されるまでに2回、ARP Requestパケットが送信されることになる。ARP Requestパケットが送信される条件を種々設定することにより、パケット通信装置A2801がエントリを削除するまでにユーザ端末2806の存在を確認する回数を調整することが可能である。

【0223】更に、パケット通信装置A2801は、ユーザ端末2806から送られてくるARP RequestパケットやARPreplyパケットによってアドレス学習テーブル2811の有効期間フィールドに保持された有効時間を更新する。パケット通信装置A2801が、ユーザ端末2806から送られてくるARPrequestパケットまたはARPreplyパケットにより、アドレス学習テーブル2811の有効期間フィールドの有効時間を更新する場合の処理を、図34を用いて説明する。

【0224】まず、ユーザ端末2806によって認証(ログイン)が行なわれたことにより、アドレス学習テーブル2811の1つのエントリには、図37に示されるようにユーザ端末2806のMACアドレス、IPアドレス、中継を示す情報、及び有効時間が登録されているとし、また、そのエントリに有効時間(300秒)が登録されてから120秒が経過しているとする。従って、アドレス学習テーブル2811のそのエントリの有効時間は180秒になっている。

【0225】パケット通信装置A2801は、ユーザ端

46

末2806から送られたARP RequestパケットまたはARPreplyパケットを受信すると、図34に示されたフローチャートに従ってARPパケット学習処理を実行する。まず、ARP RequestパケットまたはARPreplyパケットに含まれる送信元MACアドレスを対象外アドレステーブル2812から検索する(処理3401)。図31に示されている通り、対象外アドレステーブル2812にはユーザ端末2806のMACアドレスは登録されていない。そこで、パケット通信装置A2801は、その送信元MACアドレスをアドレス学習テーブル2811から検索する(処理3402)。送信元MACアドレスはユーザ端末2806のMACアドレスであり、そのMACアドレスが登録されたエントリがアドレス学習テーブル2811に存在する。よって、パケット通信装置A2801は、ARP RequestパケットまたはARPreplyパケットに含まれる送信元IPアドレスとアドレス学習テーブル2811のそのエントリに登録されたIPアドレス(147. 3. 3. 1)とを比較する(処理3405)。通常、通信中のユーザ端末2806に割り当てられたIPアドレスは変更される必要はない為、アドレス学習テーブル2811に登録されているIPアドレスと送信元IPアドレスは一致する。その結果、パケット通信装置A2801は、そのエントリに保持されている有効時間が300秒未満であれば有効時間を300秒に更新し(処理3406)、ARPパケット学習処理を終了する。この場合、有効時間は180秒である為、その有効時間は300秒に更新される。

【0226】ユーザ端末2806から送られるARP RequestパケットまたはARPreplyパケットを、パケット通信装置A2801がアドレス学習テーブル2811のエントリの有効時間の更新に利用することにより、実際にパケット通信装置A2801がARP Requestパケットをユーザ端末2806に送信する間隔は、上述した定期的な間隔(約4分)よりも長くなる。その為、ユーザ端末2806が接続されたネットワークに対する負荷が軽減される。ユーザ端末2806が通信している状態では、定期的に、または不定期にユーザ端末2806からARP RequestパケットまたはARPreplyパケットが送られてくる。その為、パケット通信装置A2801によるユーザ端末2806へのARP Requestパケットの送信は、ユーザ端末2806が通信を行わずに一定時間が経過した後、つまりユーザ端末2806がネットワークから離脱している可能性が高い状態においてのみ、ということになる。

【0227】以上の通り、ユーザが自由にユーザ端末を接続できる情報コンセントシステムを備えるネットワークシステムにおいて、パケット通信装置2801が用いられることにより、認証(ログイン)を行っていないユ

47

ユーザ端末2806のパケットは廃棄され、不正ユーザによるネットワークの利用が防止される。

# 【0228】

【発明の効果】本発明によれば、ユーザが任意の時刻及び任意の場所において情報コンセントにユーザ端末を接続しても、認証を受けたユーザのみがネットワークシステムにおけるファイルサーバ等の資源を利用でき、認証を受けていない不正なユーザによるネットワークシステムの資源の利用が防止される。

# 【図面の簡単な説明】

【図1】一実施の形態におけるパケット通信装置の構成図。

【図2】ネットワークインターフェース102～107の構成図。

【図3】アドレス学習テーブル108の構成図。

【図4】LAN100が用いられたネットワークシステムの構成図。

【図5】ユーザ端末403が情報コンセント409に接続された場合の通信シーケンス図。

【図6】LANスイッチ100の中継処理を示すフローチャート。

【図7】アドレス学習テーブル108の構成図。

【図8】図6に示された処理604のフローチャート。

【図9】中継テーブル901の構成図。

【図10】パケット通信装置の他の構成図。

【図11】フィルタリング処理部1012～1017の構成図。

【図12】フィルタリングテーブル1101の構成図。

【図13】ルータ1000が用いられたネットワークシステムの構成図。

【図14】ユーザ端末1333が情報コンセント409に接続された場合の通信シーケンス図。

【図15】フィルタリングテーブル1101の構成図。

【図16】パケット通信装置の他の構成図。

【図17】フィルタリングテーブル1607の構成図。

【図18】学習テーブル1606の構成図。

【図19】LANスイッチ1600が用いられたネットワークシステムの構成図。

【図20】ユーザ端末1905がネットワークBの情報コンセント409に接続された場合の通信シーケンス図。

(25)

特開2002-84306

48

【図21】LANスイッチ1600の中継処理を示すフローチャート。

【図22】学習テーブル1606の構成図。

【図23】ルータ2300が用いられたネットワークシステムの構成図。

【図24】ユーザ端末2312がネットワークB2313に接続された情報コンセントに接続された場合の通信シーケンス図。

【図25】ルータ2300の中継処理を示すフローチャート。

【図26】パケットを受信した認証サーバ2310の処理を示すフローチャート。

【図27】初期状態でのIPアドレス登録表2306の構成図。

【図28】複数のパケット通信装置A～C2801とルータ2820によって複数のネットワークが接続されたネットワークシステムの構成図。

【図29】サブネットテーブル2814の構成図。

【図30】認証用アドレステーブル2813の構成図。

【図31】対象外アドレステーブル2812の構成図。

【図32】パケット通信装置2801の中継処理を示すフローチャート。

【図33】ユーザ端末2806が情報コンセントシステム2830におけるネットワークに接続された場合の通信シーケンス図。

【図34】パケット通信装置2801によるARPパケット学習処理を示すフローチャート。

【図35】アドレス学習テーブル2811の構成図。

【図36】アドレス学習テーブル2811の構成図。

【図37】アドレス学習テーブル2811の構成図。

【図38】パケット通信装置2801によるアドレス学習テーブル2811の更新処理を示すフローチャート。

# 【符号の説明】

100 LANスイッチ

109 状態変更指示パケット処理部

203 状態管理部

401 認証サーバ

402 ファイルサーバ

403 ユーザ端末

409 情報コンセント

【図30】

図30

2813 認証用アドレステーブル

#	サーバアドレス
1	137.1.1.1
2	137.1.1.2
3	137.1.1.3

【図31】

図31

2812 対象外アドレステーブル  
(パケット通信装置A)

#	対象外アドレス
1	22:22:00:00:00:03

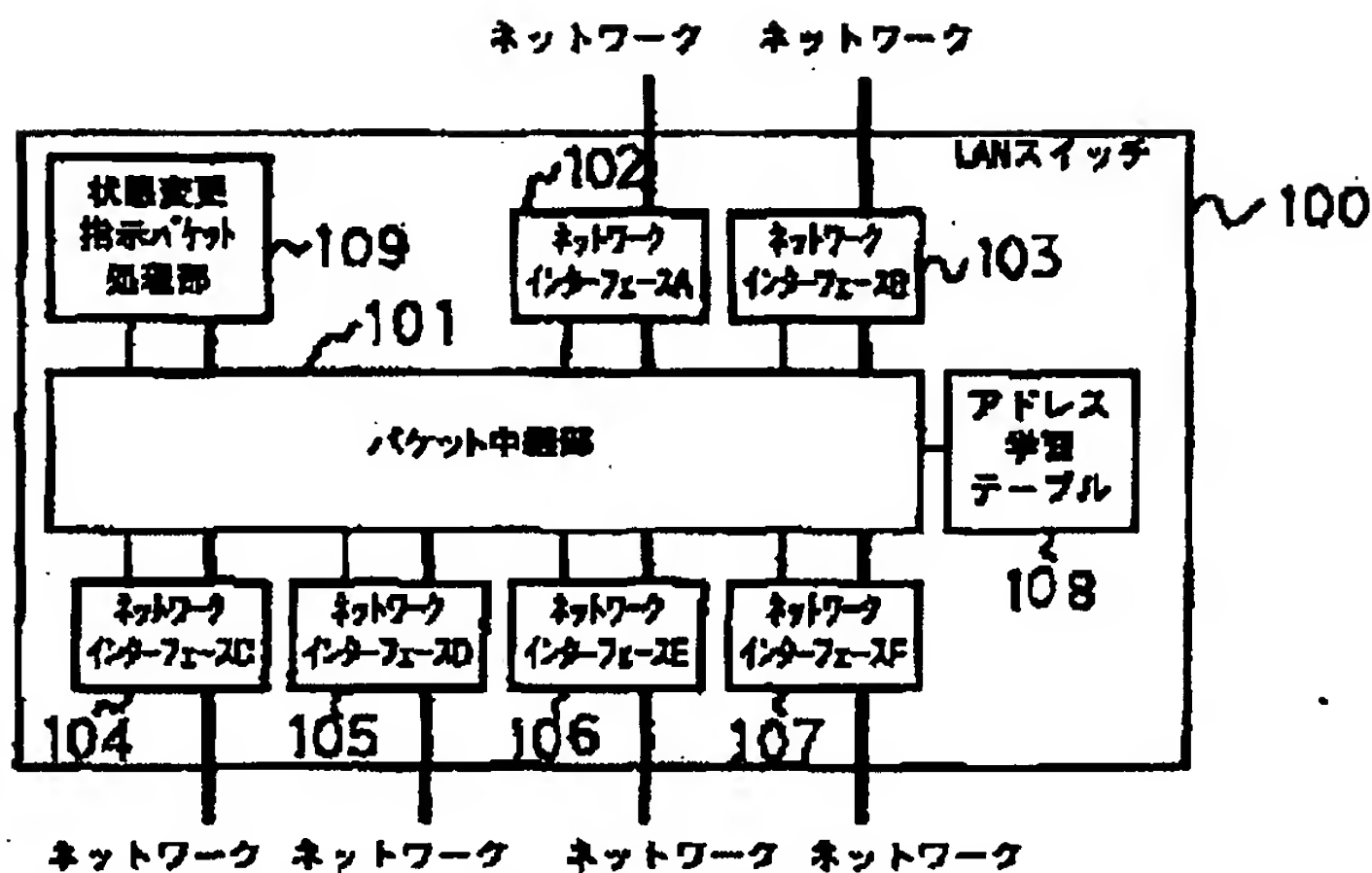


(26)

特開2002-84306

【図1】

図1



【図7】

図7

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X
4	22:22:FF:00:00:01	C

【図27】

図27

2306

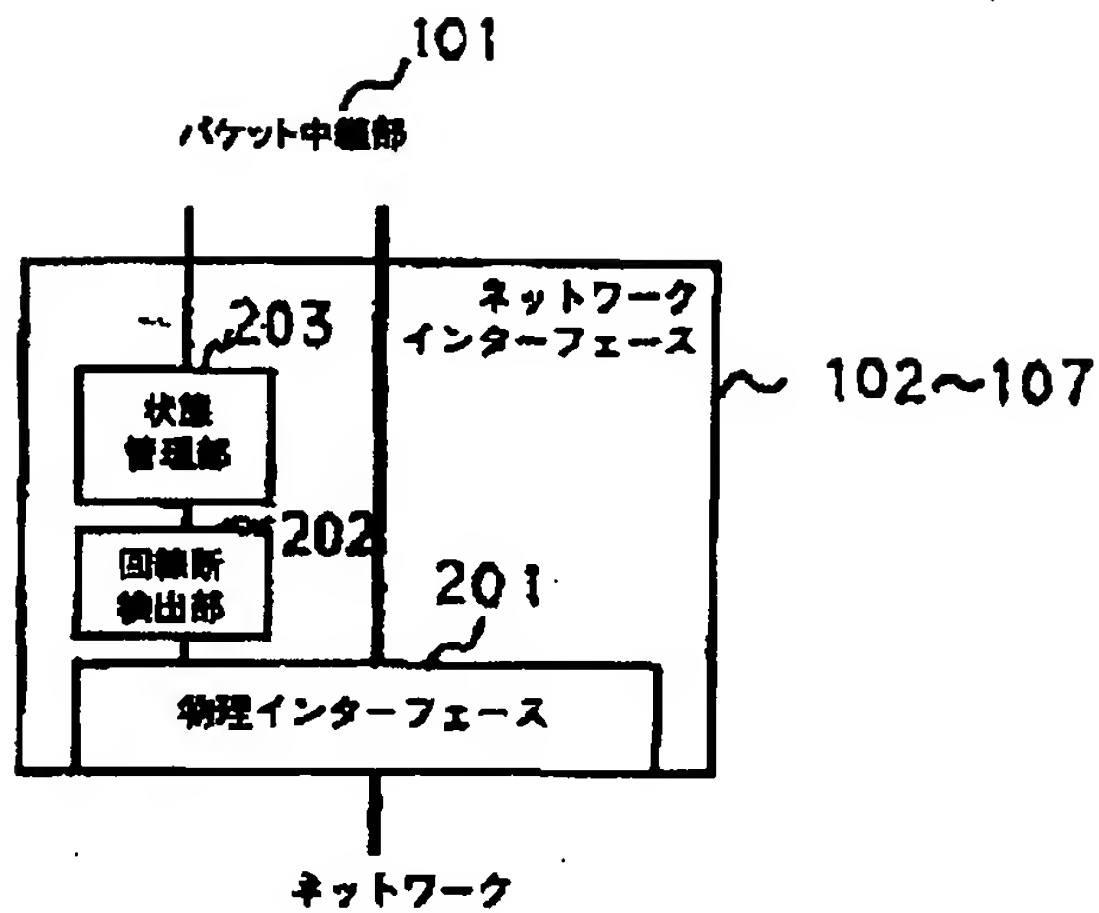
192.168.10.2
192.168.10.10

(27)

特開2002-84306

【図2】

図2



【図22】

図22

#	MAC アドレス	送信ポート
1	22:22:00:44:44:44	A
2	22:22:FF:00:00:01	B

(28)

特開2002-84306

【図3】

図3

108

301

302

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X

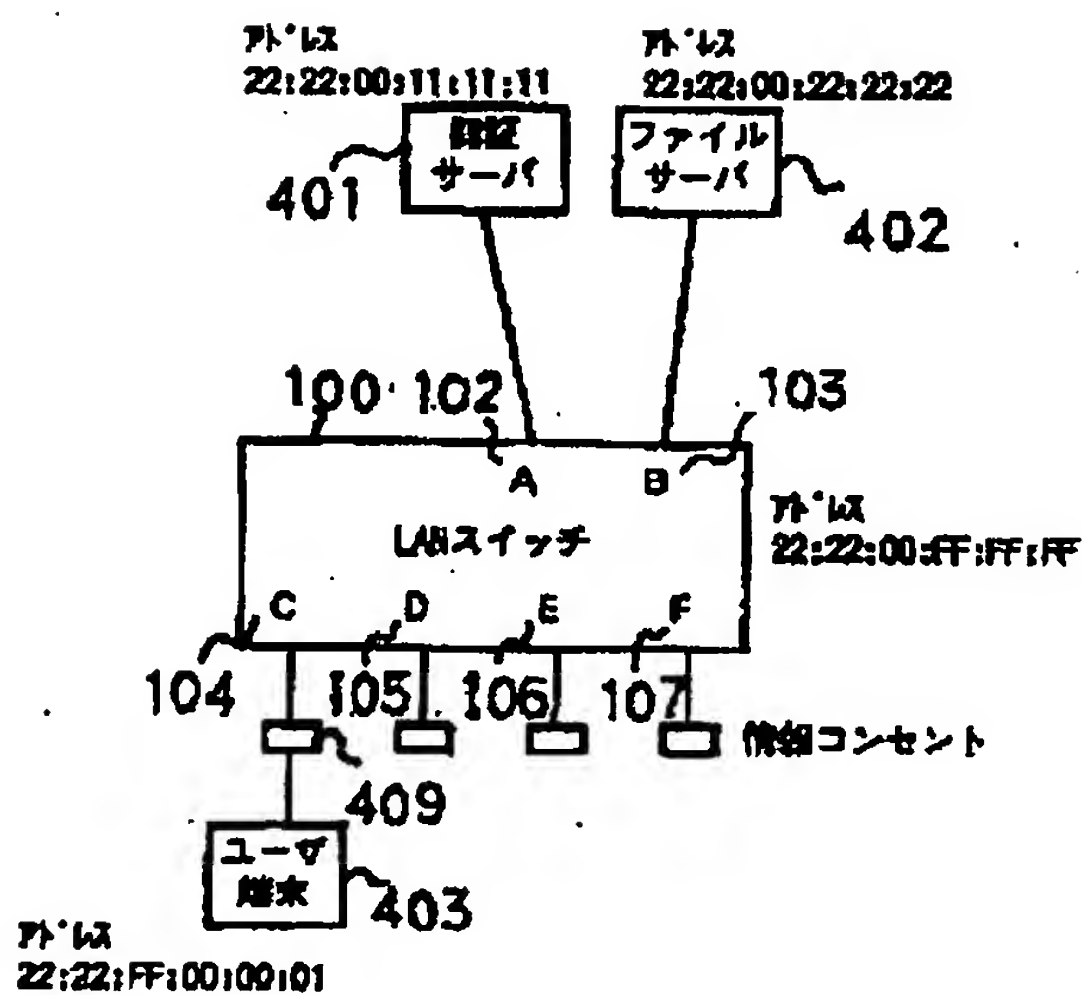


(29)

特開2002-84306

【図4】

図4



【図18】

図18

#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A

【図29】

図29

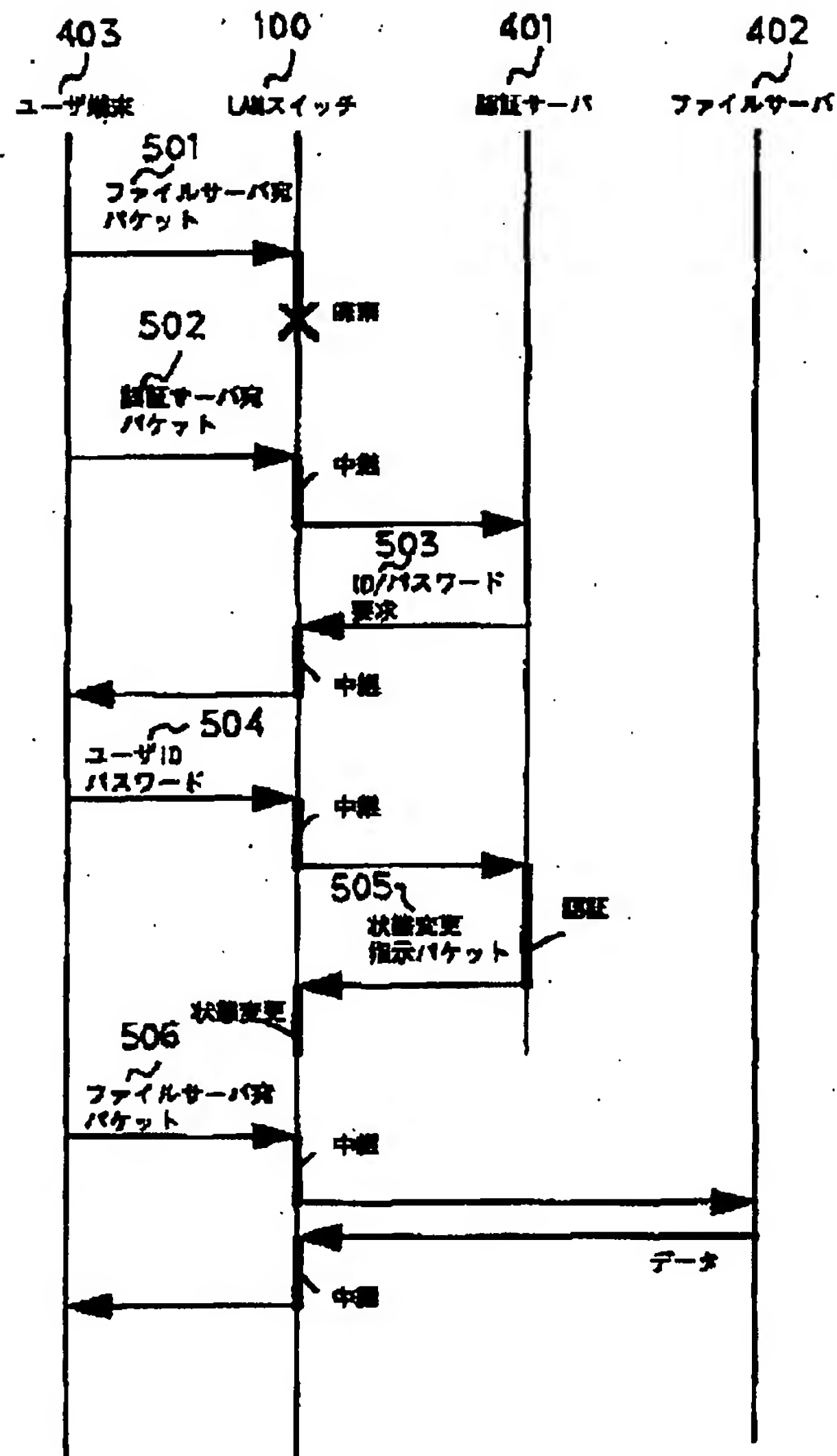
#	サブネットアドレス	サブネットマスク	フィルタリング制御装置のIPアドレス	パケット通信装置のIPアドレス
1	147.3.1.0	255.255.255.0	137.2.2.100	147.3.1.220
2	147.3.2.0	255.255.255.0	137.2.2.100	147.3.1.220
3	147.3.3.0	255.255.255.0	137.2.2.100	147.3.1.220
4	147.4.1.0	255.255.255.0	137.2.2.100	147.4.1.220
5	147.4.2.0	255.255.255.0	137.2.2.100	147.4.1.220
6	147.5.1.0	255.255.255.0	137.2.2.100	147.5.1.220
7	147.5.2.0	255.255.255.0	137.2.2.100	147.5.1.220
8	147.5.3.0	255.255.255.0	137.2.2.100	147.5.1.220

(30)

特開2002-84306

【図5】

図5

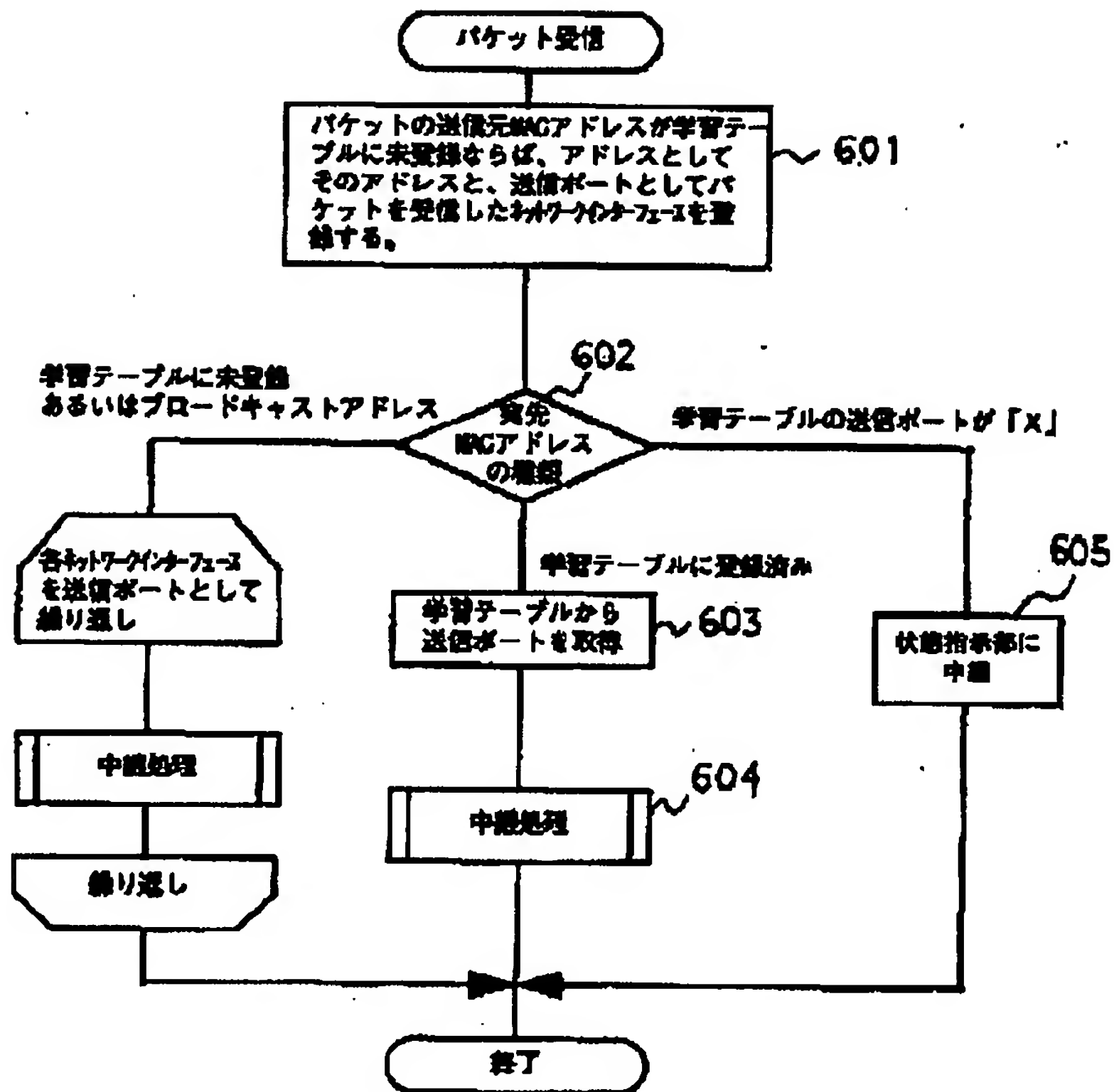


(31)

特開2002-84306

【図6】

図6



【図35】

図35

アドレス学習テーブル

#	MACアドレス	IPアドレス	状態	有効期間
1	22:22:00:11:11:11	0.0.0.0	フィルタリング ON	3600秒

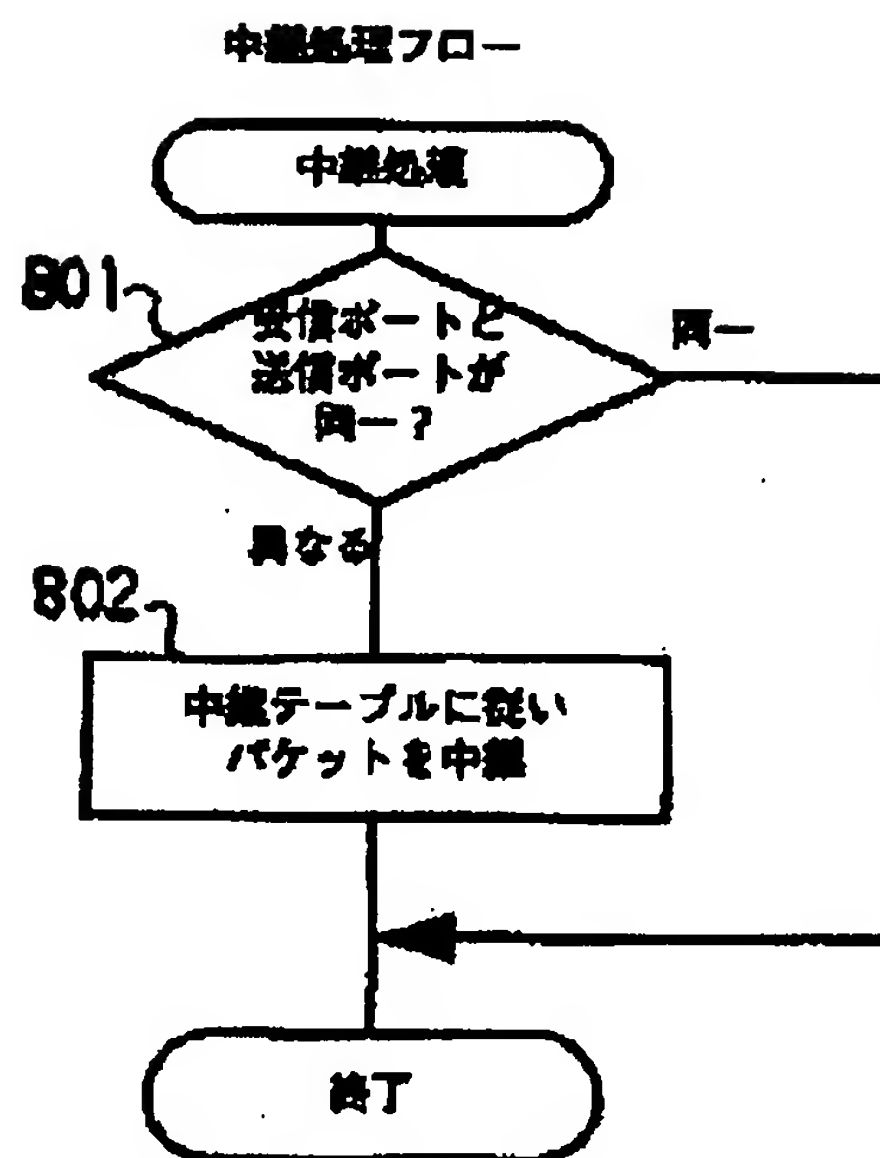


(32)

特開2002-84306

【図8】

図8



(33)

特開2002-84306

【図9】

図9

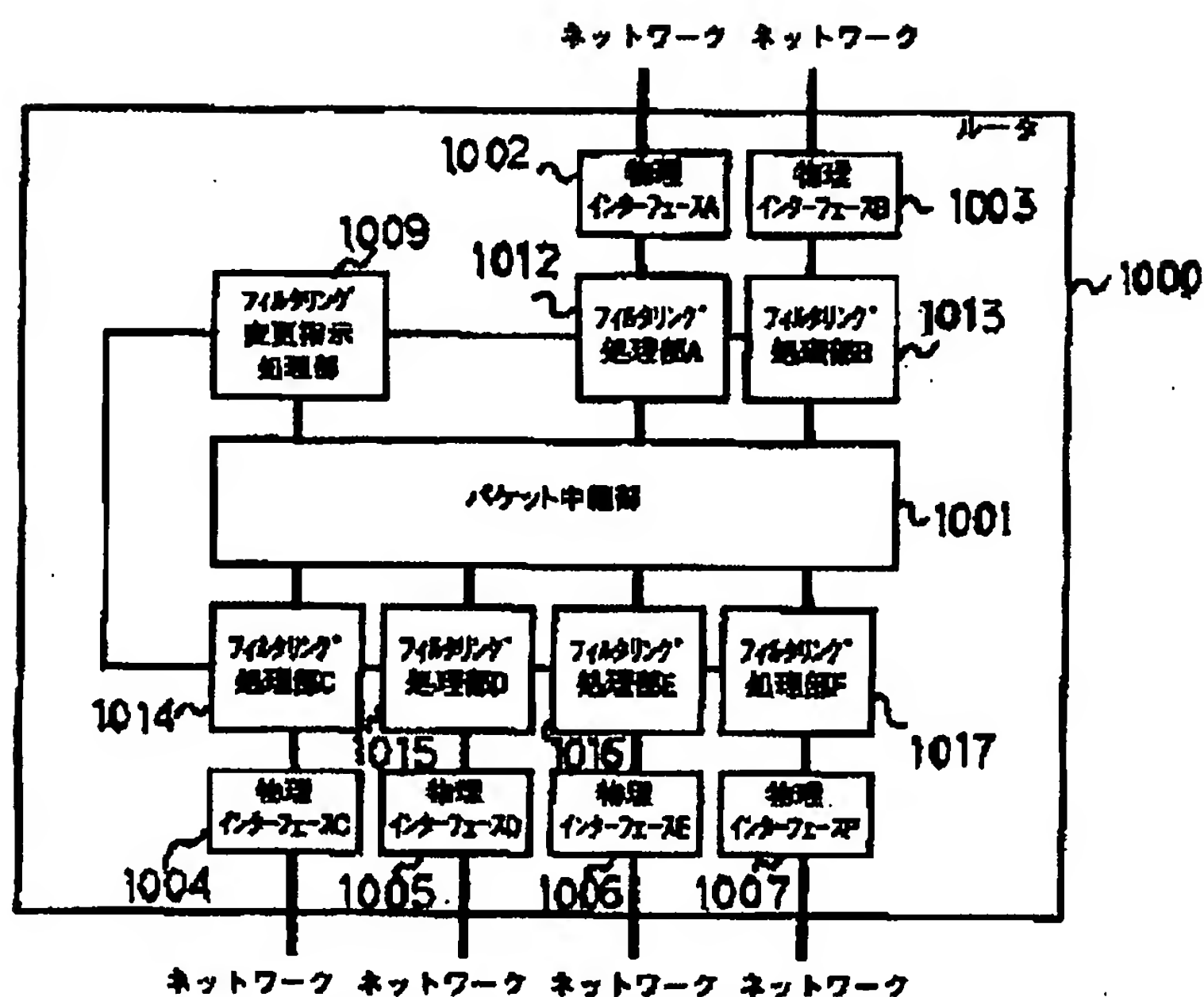
		受信ボートの状態		
		接続状態	非接続状態	状態なし
送信ボートの状態	接続状態	中継	廃棄	中継
	非接続状態	廃棄	廃棄	中継
	状態なし	中継	中継	中継

(34)

特開2002-84306

【図10】

図10



【図36】

図36

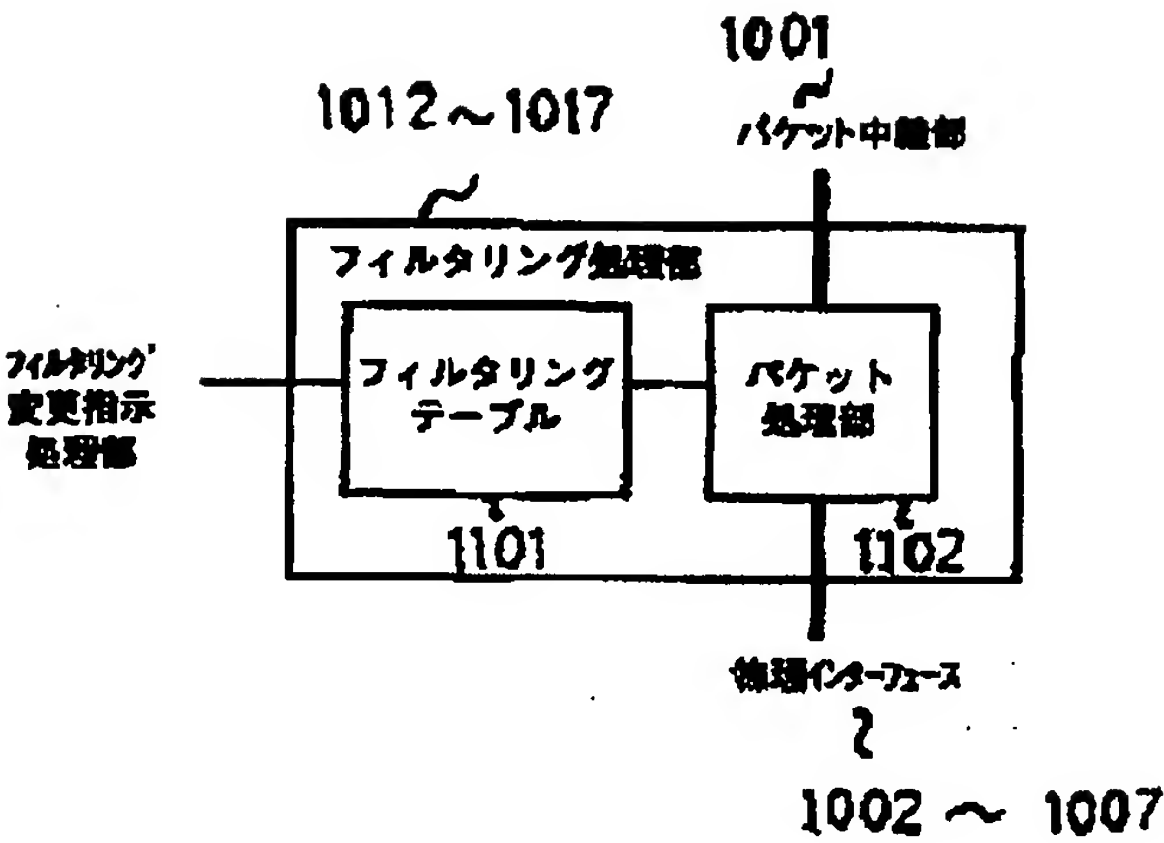
アドレス学習テーブル

#	MACアドレス	IPアドレス	状態	有効期間
1	22:22:00:11:11:11	147.33.1	フィルタリング ON	3600秒



【図11】

図11



【図37】

図37

アドレス学習テーブル

2811

#	MACアドレス	IPアドレス	状態	有効期間
1	22-22-00-11-11-11	147.33.1	フィルタリング OFF	300秒

(36)

特開2002-84306

【図12】

図12

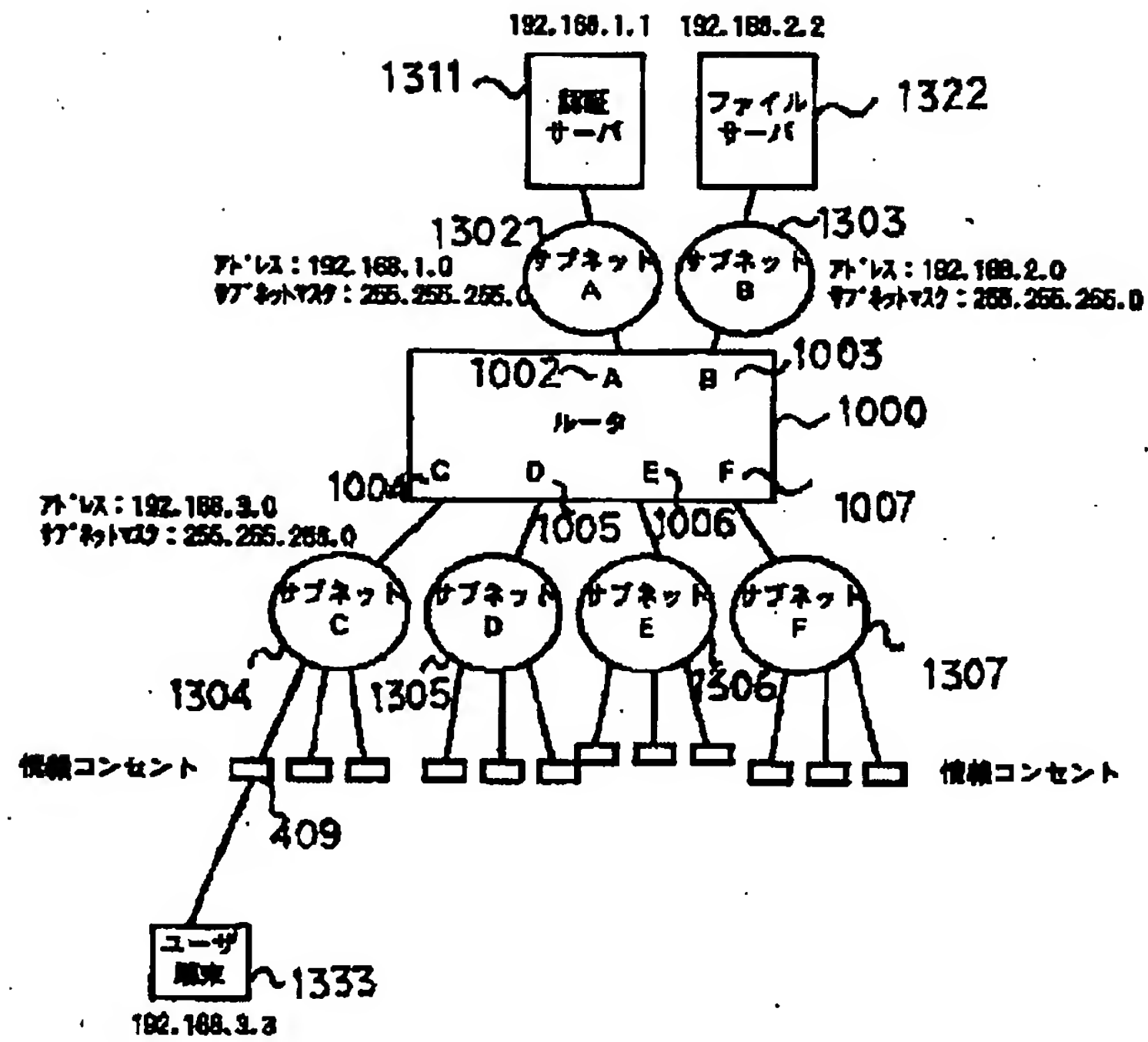
1101	1201	1202	1203
#	宛先アドレス条件	送信元アドレス条件	中継/終端フラグ
1	192.168.1.1	任意	中継
2	任意	任意	終端

(37)

特開2002-84306

【図13】

図13



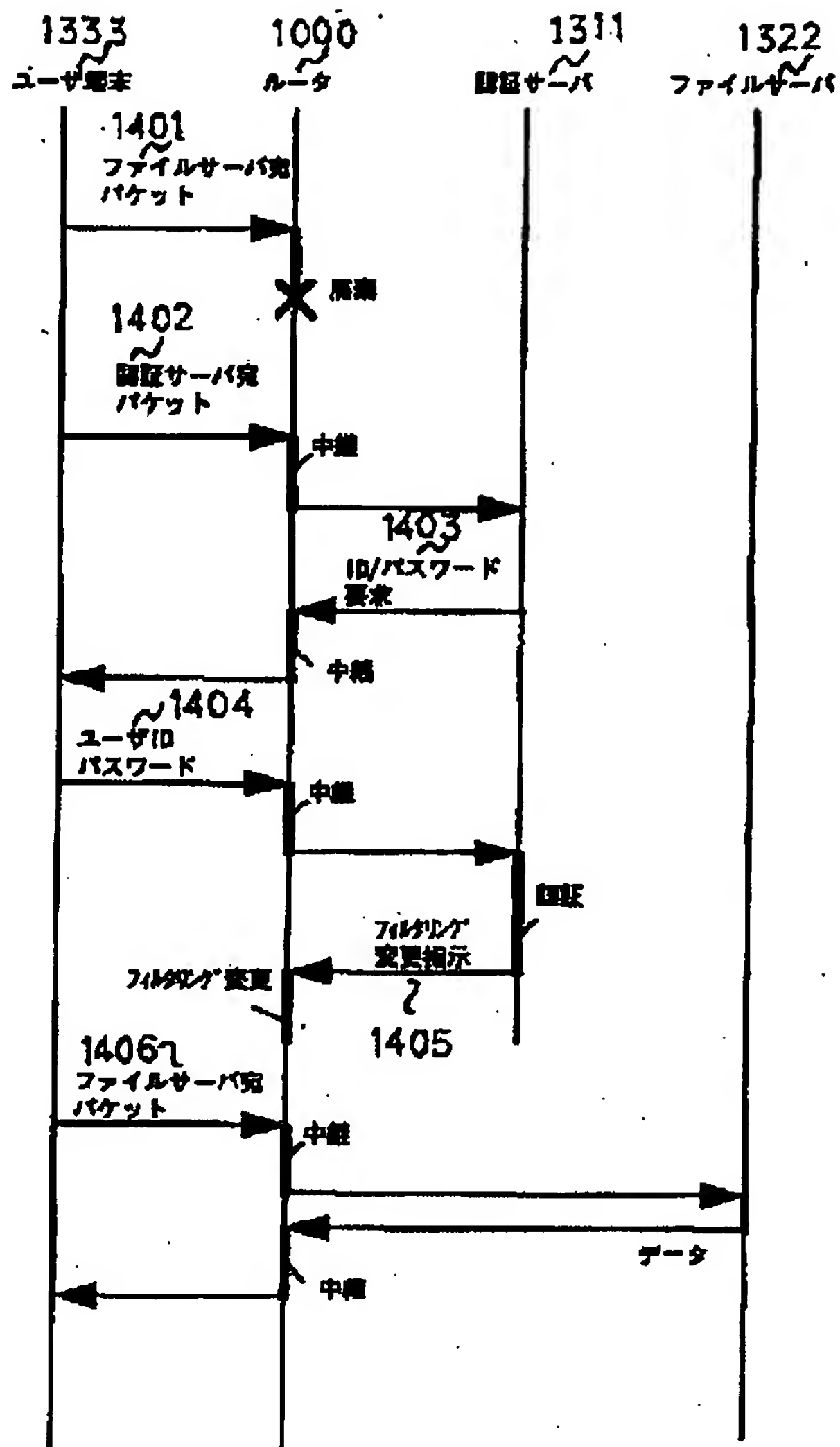


(38)

特開2002-84306

【図14】

図14



(39)

特開2002-84306

【図15】

図15

1101 7	1201	1202	1203
#	宛先アドレス条件	送信元アドレス条件	中継/転送フラグ
1	任意	192.168.3.3	中継
2	192.168.1.1	任意	中継
3	任意	任意	転送

【図17】

図17

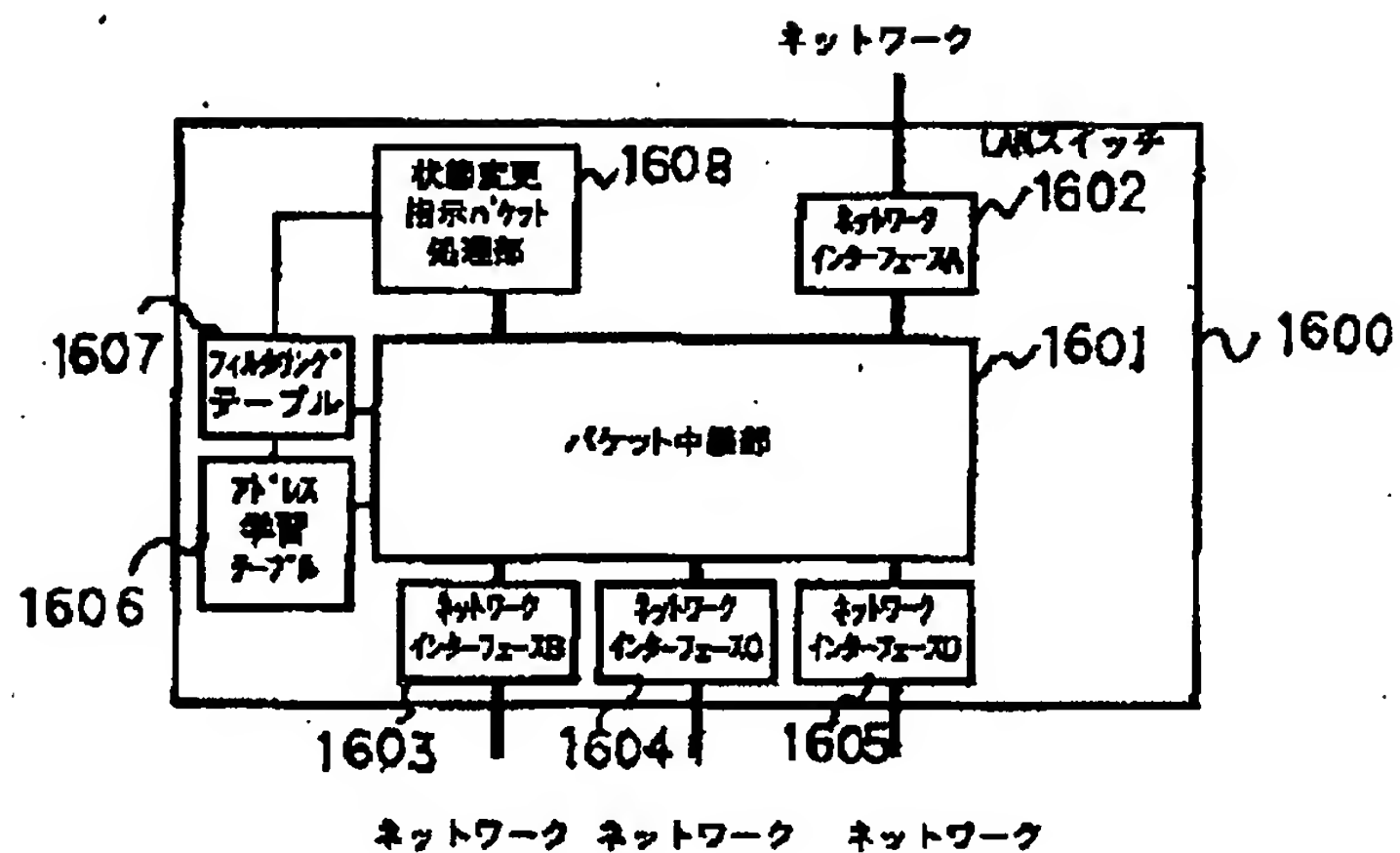
1607	1701	1702	1703
#	MAC アドレス	IP アドレス	接続ポート
1	22:22:FF:00:00:01	未登録	B

(40)

特開2002-84306

【図16】

図16

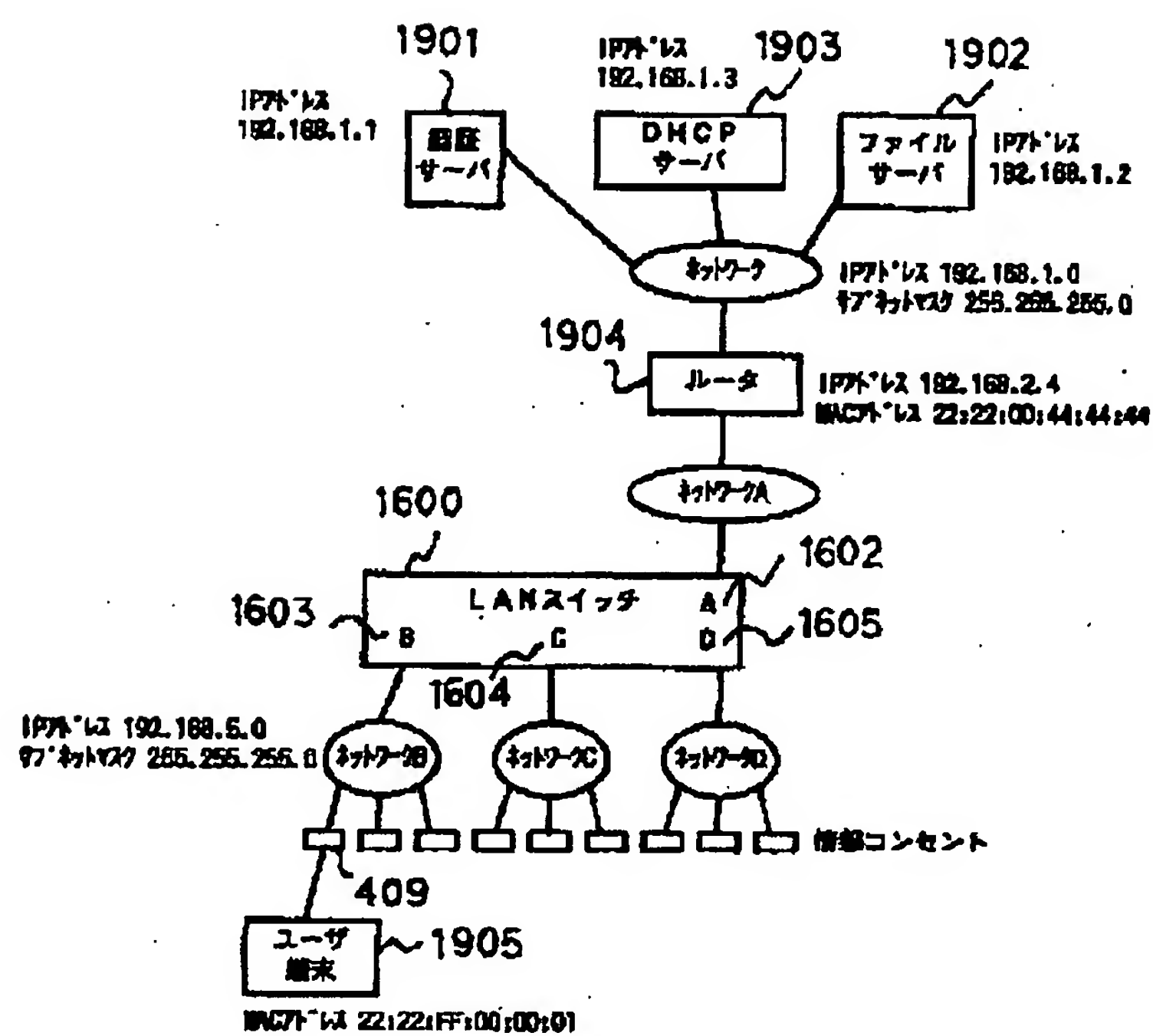


(41)

特開2002-84306

【図19】

図19



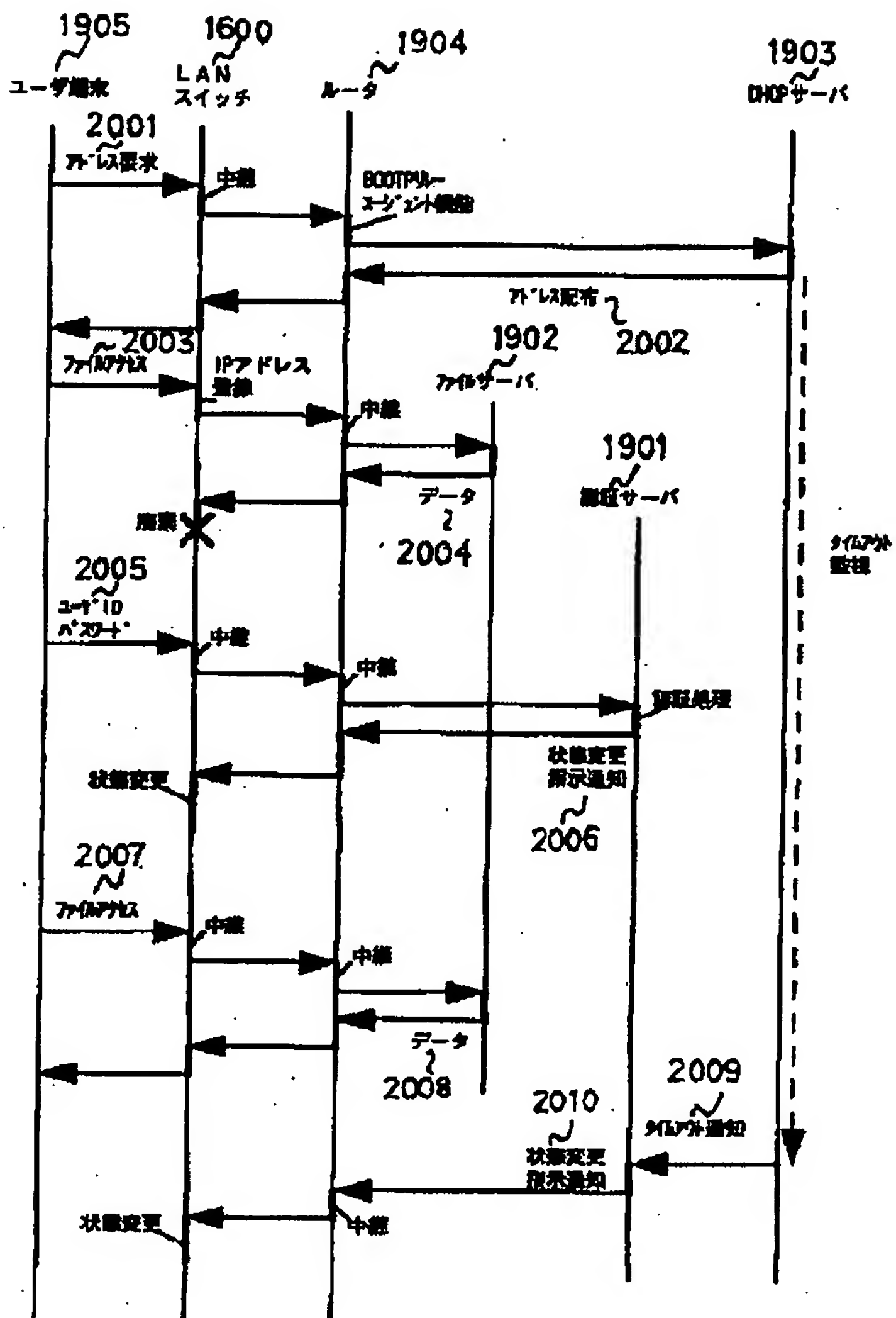


(42)

特開2002-84306

【図20】

図20

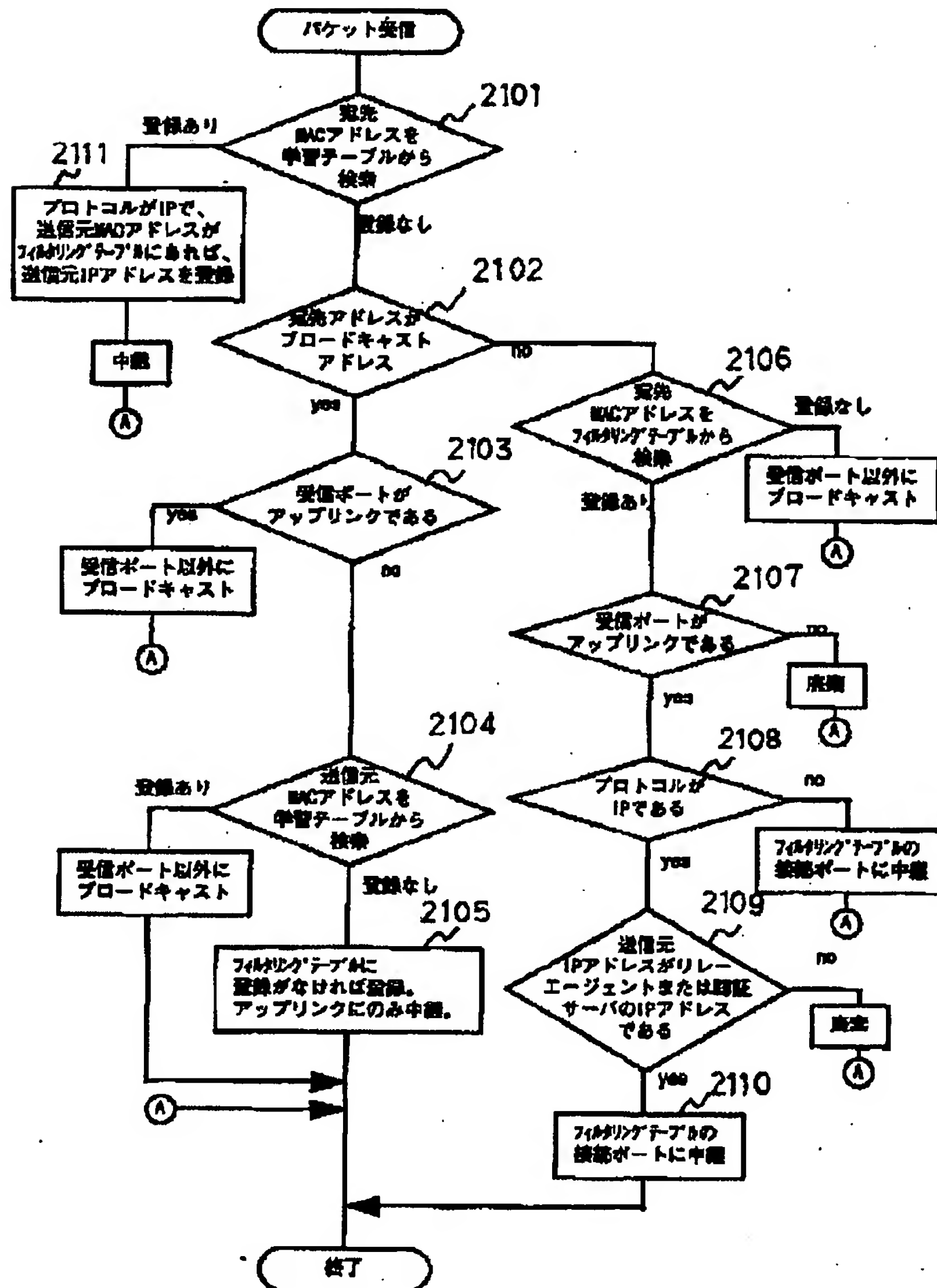


(43)

特開 2002-84306

【図 21】

図 21

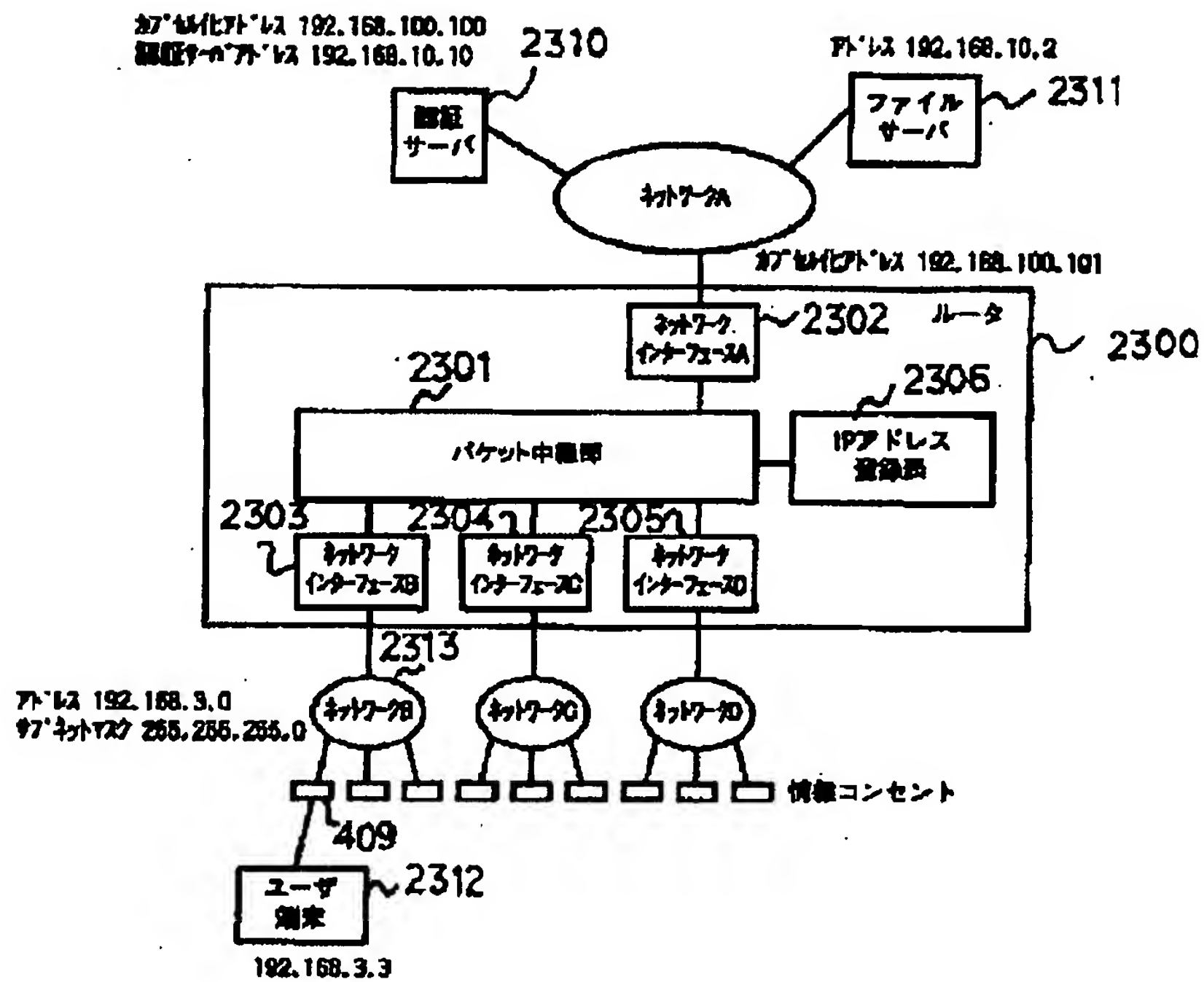


(44)

特開2002-84306

【図23】

図23

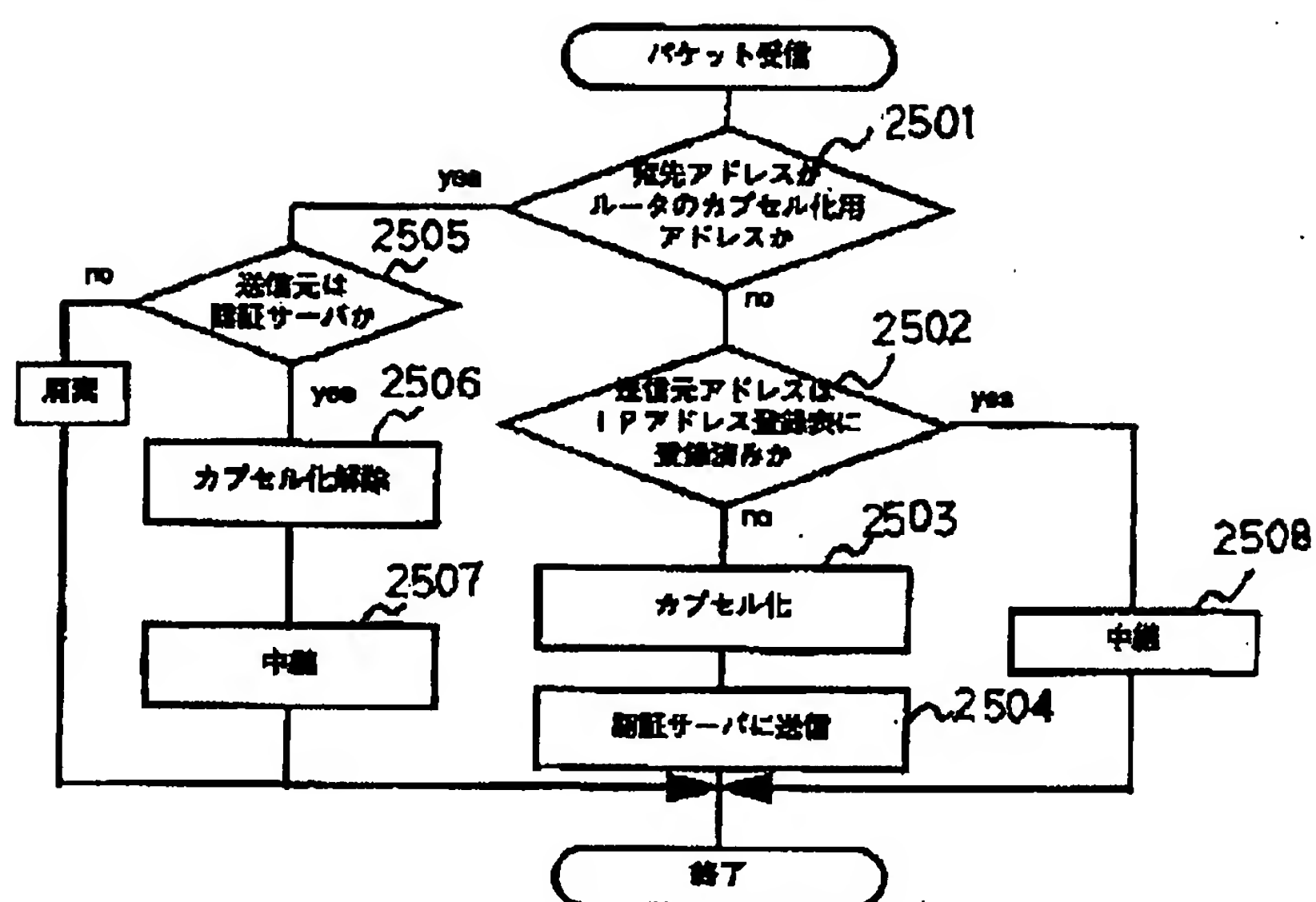


(46)

特開2002-84306

【図25】

図25



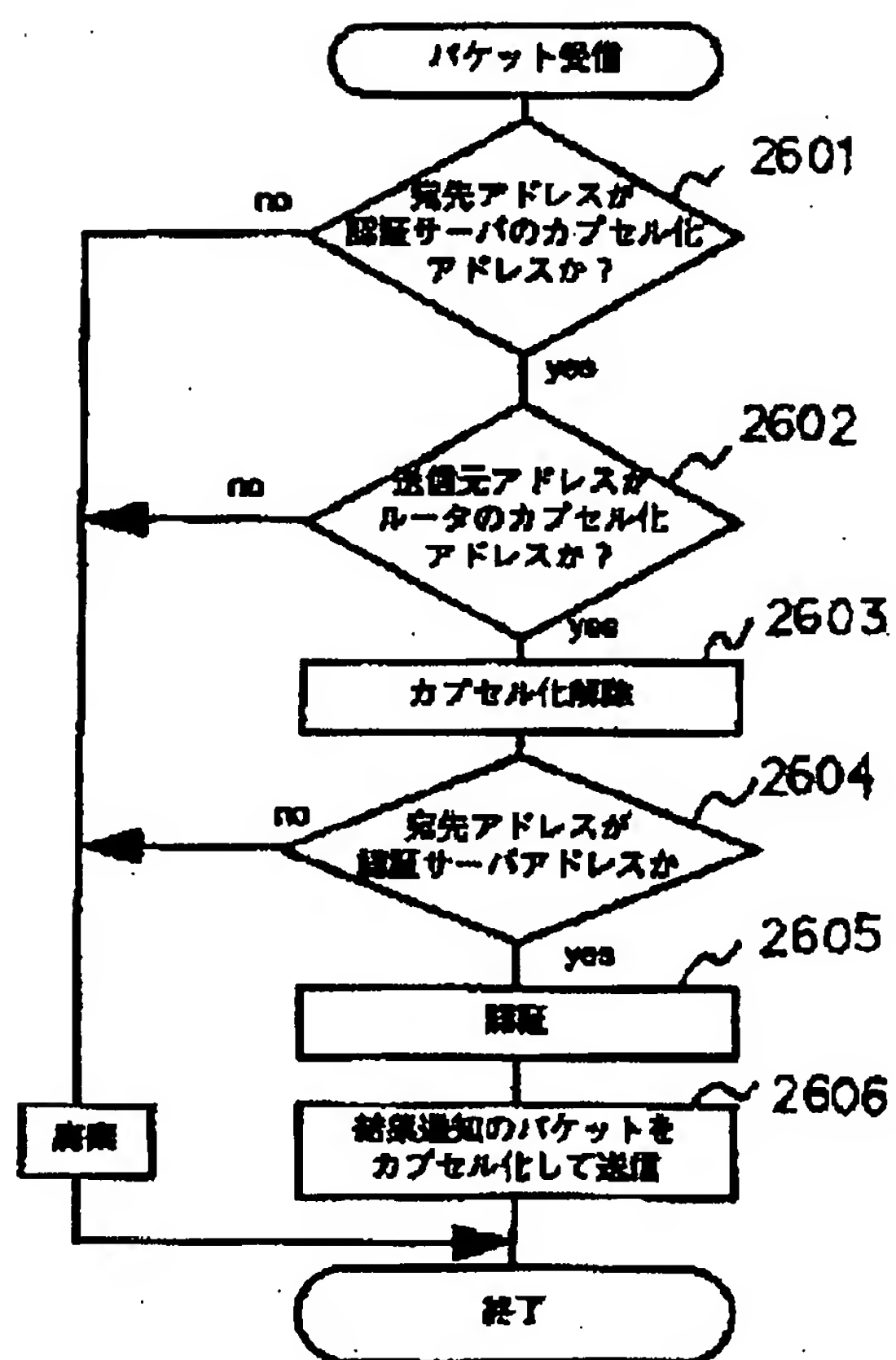


(47)

特開2002-84306

【図26】

図26

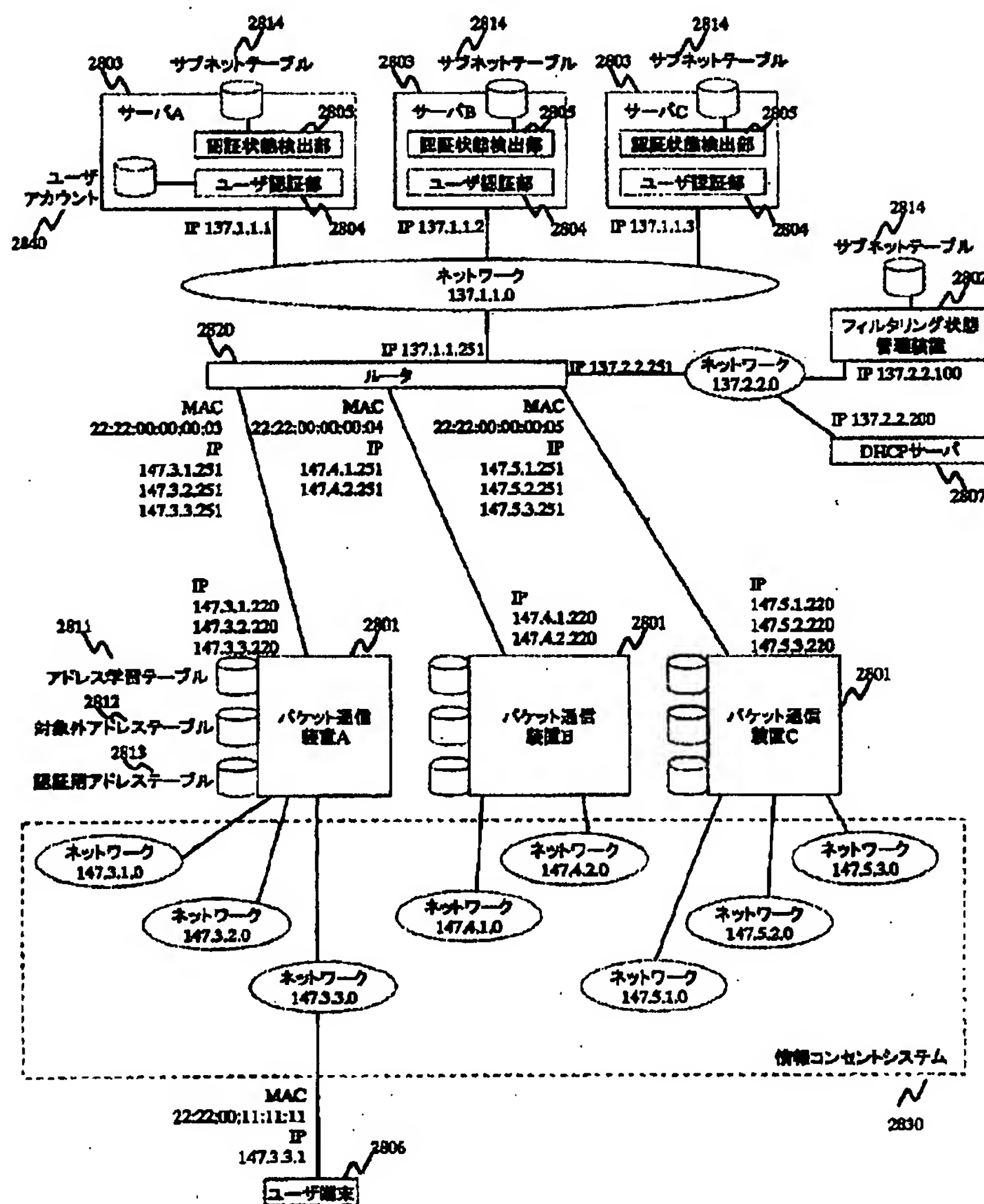


(48)

特開2002-84306

【図28】

図28

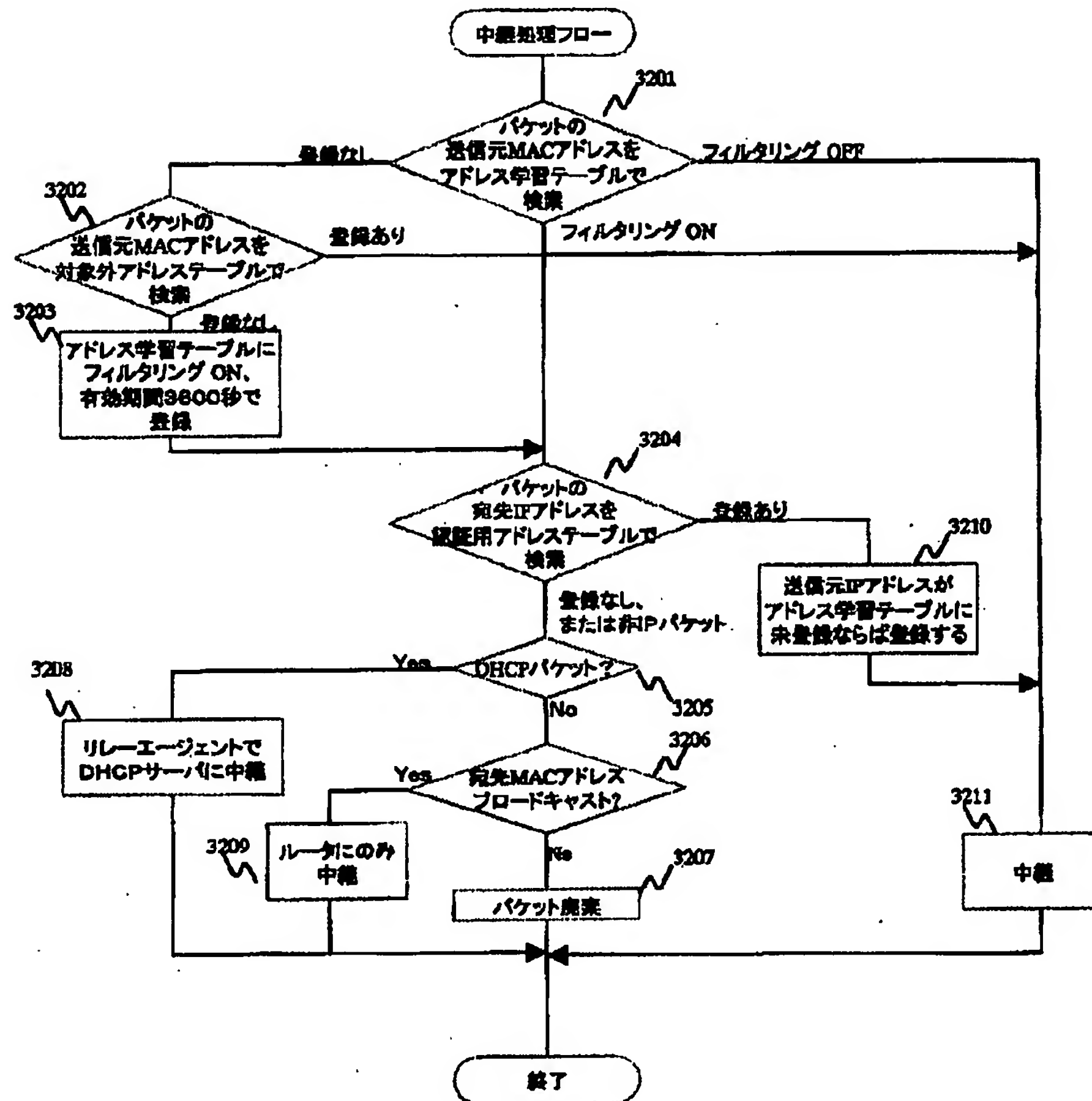


(49)

特開2002-84306

【図32】

図32

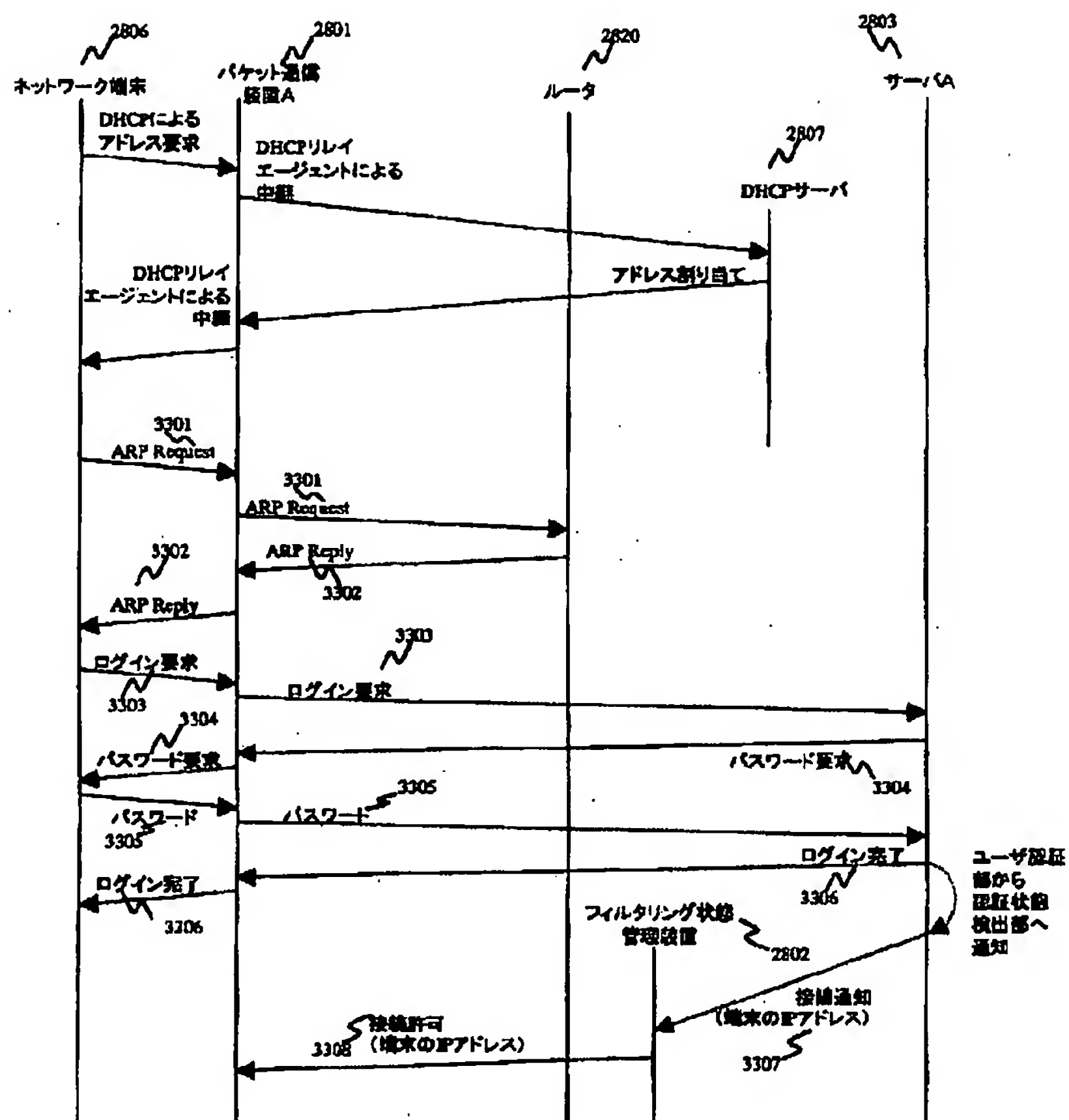


(50)

特開2002-84306

【図33】

図33



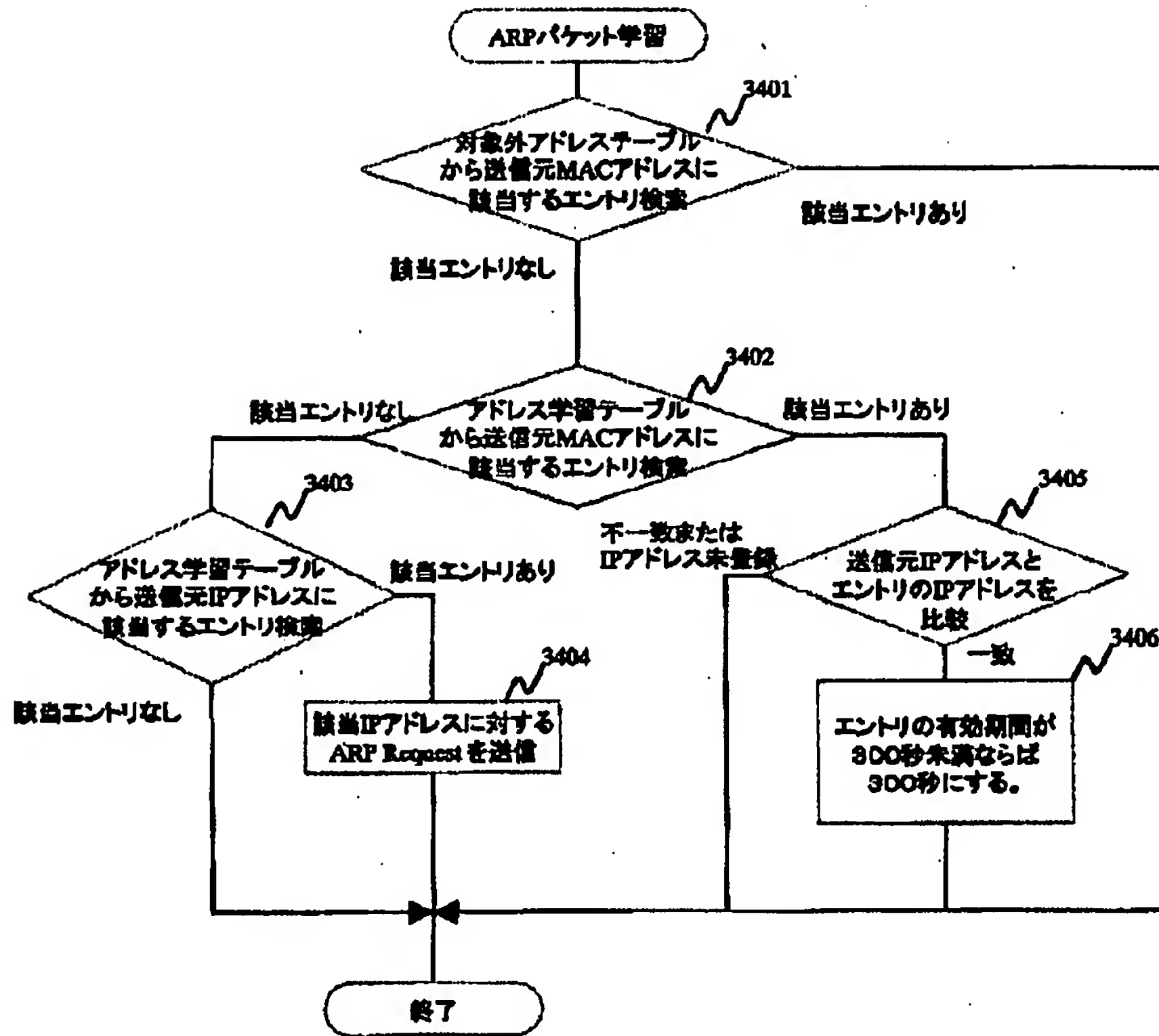


(51)

特開2002-84306

【図34】

図34

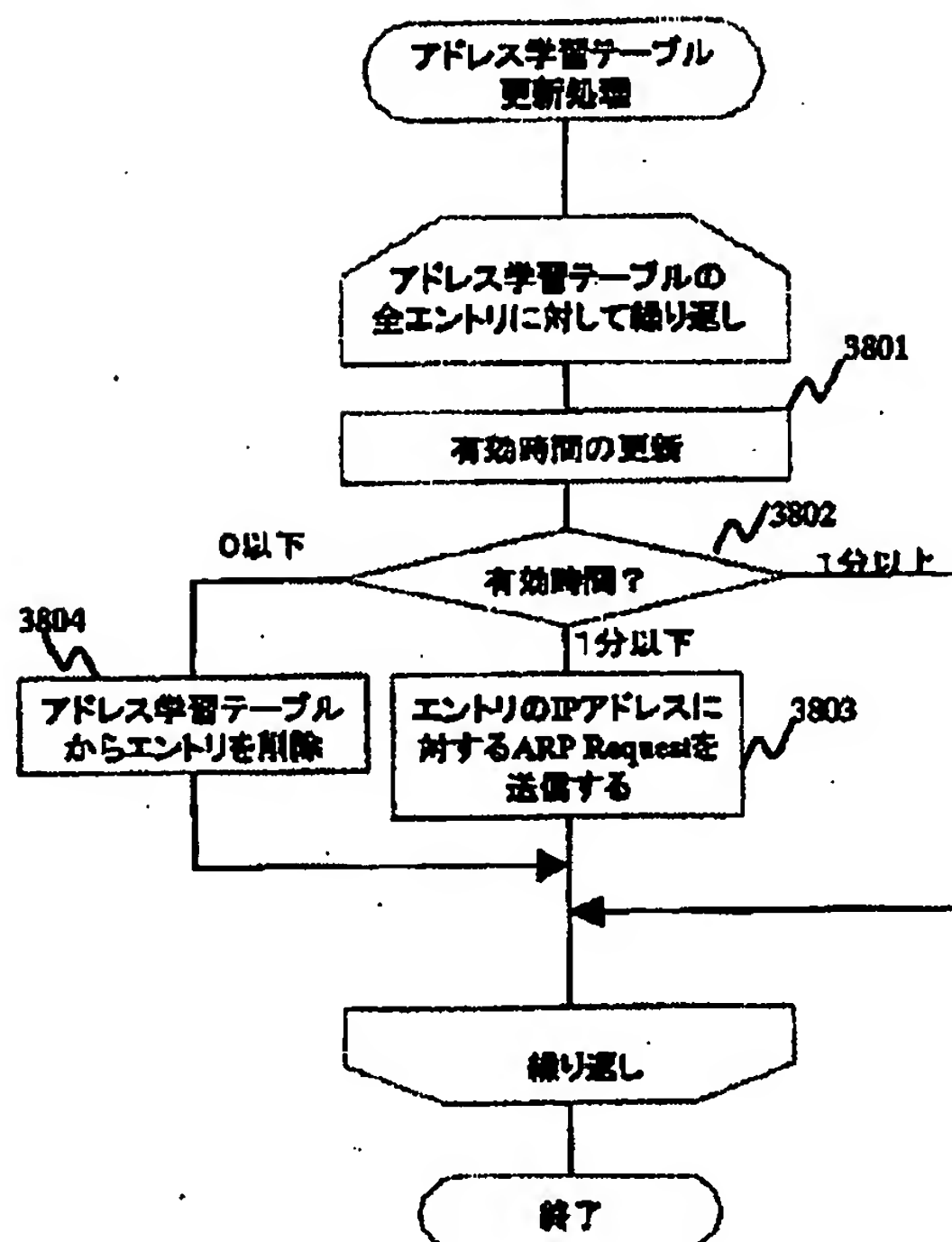


(52)

特開2002-84306

【図38】

図38



フロントページの続き

(51) Int. Cl.<sup>7</sup>

H04L 12/56

識別記号

100

F I

H04L 12/56

テーマコード(参考)

B

1002

(72) 発明者 野崎 信司

神奈川県秦野市堀山下1番地 株式会社日  
立製作所エンタープライズサーバ事業部内

(72) 発明者 巽 義行

東京都江東区新砂一丁目6番27号 株式会  
社日立製作所公共システム事業部内

Fターム(参考) 5K030 GA15 HA08 HB18 HC14 HD03

HD07 HD10 KA05 KA13 KX24  
LB05 LC13 LD20

5K033 AA08 CB01 CB08 CC01 DA01

DA05 DB12 DB19 EA07 EC01

EC04